ISSN 0956-9979 MARCH 1997

# VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL



## IN THIS ISSUE:

• **In a *Word*...** What is the likelihood of *WordBasic* macro viruses propagating successfully under *Word 97*? *VB* discusses the issue. Turn to p.6 for the story.

• **Down a new path.** TPVO reflects a new development in virus creation: not just bi-, but tri-partite, this virus can infect boot sectors as well as DOS and *Windows* executables. Analysis on p.8.

• ***NetWare* once more.** It's that time of year again, when one's thoughts turn to reviewing *NetWare* anti-virus products. Turn to page 10 to find out what happened.

## CONTENTS

# EDITORIAL

## Blissful Ignorance...

*“Bliss is not a problem, but just may be the precursor to something that is...”*

It has been an interesting month for someone with similar professional interests as my own – finally, after such a long time (in computing terms at least), viruses meet Linux in the real world! For those readers looking blankly at the page wondering what on earth I mean, Linux is the pinnacle of the freeware ethic – a complete, and completely free, UNIX clone. Originally for *Intel* 386 and above computers, versions are now available for *Sun SPARC*, *DEC Alpha*, and *Power PC*. Supported by the GNU toolset, it is the choice of the discerning, but spendthrift, administrator of small-to-medium-sized WWW and FTP servers. Supported by developers world-wide, Linus Torvalds (the system's creator) produces frequent kernel upgrades containing fixes and new features.

But, wait! It's a UNIX, for heaven's sake! Everybody knows native UNIX viruses are a non-threat, right? I mean, sure – you have to watch out for DOS viruses being transferred across your UNIX fileserver, but that's about it.

One of the most compelling reasons for the lack of a virus problem in the UNIX world is the large number of different, and mutually incompatible, flavours of UNIX. If I use *Solaris*, I cannot pass executables to friends running any other type of UNIX. Certain types of 'executable' are interchangeable, of course – most UNIX machines must have a copy of 'sh' (the Bourne Shell), and a high percentage will have perl, but, in terms of raw executables, and unlike DOS, exchangeability is very low.

However, users of any one flavour can exchange binary executables, and there are many Linux users out there. Not only that, the type of person who uses Linux is also the type who passes software around a lot; he likes to play with computers. This type of person is also much at risk from viruses – all that software passing from hand to hand. Finally, Linux users often do their work from the administrative account, making it easy for a virus to infect whatever programs it wishes.

Anyway, to return to the story, in early February something went rotten in the state of Linux. A message was posted to a computer security mailing list called BugTraq, from a Linux user who reported being infected by the Bliss virus. Research revealed that the virus was first released in mid-1996 – at that time, clearly labelled as a virus. Various versions have circulated quietly in Linux circles since then, but it is only now that the virus actually appears to have generated infections in the real world.

Someone on the BugTraq list passed the news to researchers at *McAfee*, who swiftly examined the virus and built detection for it into their DOS and Linux products. Bliss (otherwise known by the catchy name of Linux/HLLO.17892) is extremely easy to detect – it simply overwrites target programs with the constant stream of bytes that make up the virus code.

Immediately after these developments on BugTraq, *McAfee's* marketing department produced a press release stating: '*McAfee* discovers first Linux virus'! Perhaps '*McAfee* handed marketing opportunity on a platter' would have been more appropriate; after all, it is not as if the 'discovery' was down to them. Neither is it the first Linux virus – at least one other springs to mind, published in VLAD a while back (admittedly, that only worked on one particular kernel revision). Apart from this, Fred Cohen demonstrated functional UNIX viruses in the early 1980s which would work perfectly well on modern Linux systems.

However, leaving aside my now-trademark griping about the language of the press release, there is a real risk here. Despite the fact that Bliss is incredibly obvious once it has infected your system, Linux users are, basically for the first time, at risk from a virus. Can it be that the virus world is changing again? We all remember how things changed when Concept appeared – are we about to face another such shift? The answer is surely 'not yet': Bliss is not about to rampage across the Linux world, destroying all in its way. It is so noticeable on an infected system (not a single infected object works as expected when run!) that there is no way it can survive for long in the user community.

Nevertheless, it pays to remember an old saying: 'tall oaks from little acorns grow.' Bliss is not a problem, but just may be the precursor to something that is…

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**

# NEWS

## VB'97: Be Sure to Wear Some Flowers in your Hair

California, home to the famous Silicon Valley, has been selected as the venue for this year's *Virus Bulletin Conference*. *VB'97* will take place on 2/3 October 1997 at the *Fairmont Hotel*, atop San Francisco's Nob Hill.

The *VB* conference is the world's foremost anti-virus gathering, and has a well-deserved reputation for delivering high quality papers and debate whilst at the same time having a social programme second to none.

Response to the call for papers was quick and plentiful, meaning that the conference programme is already being finalised – *VB* subscribers can expect to receive their copy within the next couple of months. All conference information will also be published on the *Virus Bulletin* WWW site (http://www.virusbtn.com/) as it becomes available.

The two-day conference will return to its regular format of one technical and one corporate stream running parallel presentations, and papers will be given by the world's leading anti-virus researchers. Also featured will be the developers' exhibition, now in its fourth year, and an established part of the proceedings – the regular quota of major anti-virus vendors is expected to participate.

Readers wishing to register or obtain further information may contact Alie Hothersall at the *Virus Bulletin* offices; tel +44 1235 555139, fax +44 1235 531889, email alie@virusbtn.com ▮

## Cry 'Wolf'!

In recent months, the number of calls to *Virus Bulletin* concerning non-existent viruses (viz hoaxes) has risen once more. There are several which fall into this category, and readers are advised again that reports of the 'viruses' listed below are false, and should be ignored.

The classic Good Times spawned many variant warnings, including Penpal Greetings, Deeyenda Maddick, Goblyn, and Join the Club (also known as Join the Crew). Apart from this particular family of hoaxes, *Virus Bulletin* is aware of one other 'non-virus' – Irina – which was started as a publicity stunt to advertise an electronic novel.

The hoaxes mentioned above had many things in common, primarily the fact that they all refer to transferring themselves automatically by email to people who exchange mail. This type of spread is not possible under today's wide variety of email utilities and operating systems. Readers who are uncertain whether or not virus warnings are plausible from a technical point of view may contact our helpline; +44 1235 555139, or email editorial@virusbtn.com ▮

### Prevalence Table – January 1997

| Virus | Type | Incidents | Reports |
|---|---|---|---|
| Concept | Macro | 93 | 18.5% |
| NPad | Macro | 38 | 7.5% |
| AntiEXE.A | Boot | 36 | 7.1% |
| Form.A | Boot | 33 | 6.5% |
| Wazzu | Macro | 28 | 5.6% |
| AntiCMOS.A | Boot | 24 | 4.8% |
| Parity_Boot.B | Boot | 22 | 4.4% |
| Empire.Monkey.B | Boot | 15 | 3.0% |
| NYB | Boot | 14 | 2.8% |
| Junkie | Multi | 13 | 2.6% |
| Ripper | Boot | 13 | 2.6% |
| WelcomB | Boot | 12 | 2.4% |
| MDMA | Macro | 9 | 1.8% |
| Stoned.Angelina | Boot | 8 | 1.6% |
| Johnny | Macro | 8 | 1.6% |
| MDMA.B | Macro | 8 | 1.6% |
| Sampo | Boot | 7 | 1.4% |
| Stealth_Boot.B | Boot | 7 | 1.4% |
| Jumper.B | Boot | 6 | 1.2% |
| Quandary | Boot | 6 | 1.2% |
| Manzon | File | 5 | 1.0% |
| V-Sign | Boot | 5 | 1.0% |
| Helper | Macro | 5 | 1.0% |
| Natas.4744 | Multi | 4 | 0.8% |
| One_Half.3544 | Multi | 4 | 0.8% |
| Showfxx | Macro | 4 | 0.8% |
| Da'Boys | Boot | 3 | 0.6% |
| DelCMOS.B | Boot | 3 | 0.6% |
| Leandro | Boot | 3 | 0.6% |
| Stoned.Spirit | Boot | 3 | 0.6% |
| TPVO.3783 | Multi | 3 | 0.6% |
| Laroux | Macro | 3 | 0.6% |
| Other[1] | | 59 | 10.9% |
| Total | | 504 | 100% |

[1] The Prevalence Table includes two reports of each of the following viruses: Bandung, Colors.A, Colors.B, EXEBug.A, Hybrid, Int40, Russian Flag.A, Stat, Stoned.Manitoba, Tequila, Yale. The table also includes one report of each of the following: Alien, AntiCMOS.B, BatMan.2844, Boot.437, Burglar.1150, BW.1287, Cascade.1701, Delwin.1759, Die_Hard, Edwin, Hare.7601, Havoc.3072, Imposter, Irish, Joshi, Kompu, Major.1644, Michelangelo.A, Nightfall.4518.B, Parasite.903, Pasta, Pindonga, Rhubarb, Satria.A, Stealth_Boot.I, Stoned.Diablo, Stoned.NoInt, Stoned.NOP, Stoned.Spirit, Swiss_Boot, Telefonica, Trackswap, Trojector.1463, Trojector.1561, Tubo, Unashamed, and Urkel.

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**

# IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 21 February 1997. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

**Type Codes**

- **C** Infects COM files
- **D** Infects DOS Boot Sector (logical sector 0 on disk)
- **E** Infects EXE files
- **L** Link virus
- **M** Infects Master Boot Sector (Track 0, Head 0, Sector 1)
- **N** Not memory-resident
- **P** Companion virus
- **R** Memory-resident after infection

**Afori.656**

**CER:** An appending, 656-byte virus containing the plain-text string: 'A41a5'. Infected COM files start with byte 27h; EXE files have the byte 1Ah located at offset 14h. The virus payload consists of sound and a 'Cascade'-like effect of falling letters.

```
Afori.656          6006 1E05 00B5 7403 E9E3 00B8 2435 CD21 520E 1FBA A800 B824
```

**Elvira.240**

**CN:** An appending, 240-byte direct infector which avoids infecting files shorter than 4096 bytes. All infected files have their time-stamps set to 62 seconds.

```
Elvira.240         B440 B9F0 008D 54FD 90CD 215A 5980 C91F B801 57CD 21E8 0900
```

**Fricker.395**

**CN:** An appending, 395-byte direct infector. Between 8:00 and 9:00 am it displays the message: 'FRICKER-1 is glad to meet YOU!'.

```
Fricker.395        B43F B901 00BA D000 CD21 3E80 3ED0 0024 7514 B43E CD21 3E80
```

**Kassasin.845**

**CER:** An appending, 845-byte virus which contains the text: ' [The ASSASSIN (Type A)] 95-03-02 (c) Copyleft 9188-9192 by SVS,Corea'.

```
Kassasin.845       B430 80C4 50B0 F086 E0CD 210B C074 51BF 611E 4FFC 9075 FB1E
```

**Kassasin.850**

**CER:** An appending, 850-byte minor variant of the above virus. It contains exactly the same text.

```
Kassasin.850       B430 80C4 50B0 F086 E0CD 210B C074 52BF 611E 4FFC 9075 FB1E
```

**Lauren**

**CN:** A family of appending, direct infectors containing the same text: '[Lauren] Virus 0.1b Dedicated with love to Lauren.... Have fun in NYC sweetums!!! *snuggles* Love, Cody', '*.COM' and 'TBAV'.

```
Lauren.632         81ED 0A01 BF00 018D B667 03FC A5A5 A5A4 B8FF FF50 58FA 83EC
Lauren.652         81ED 0A01 BF00 018D B67B 03FC A5A5 A5A4 B8FF FF50 58FA 83EC
Lauren.653         81ED 0A01 BF00 018D B67C 03FC A5A5 A5A4 B8FF FF50 58FA 83EC
```

**Predator.1060**

**CR:** A stealth, encrypted, appending, 1060-byte virus containing the texts 'Predator virus (c) Mar. 93 Priest' and '.COM'.

```
Predator.1060      BA06 02B1 ??FA 8BEC BC?? ??58 F7D0 D3C8 50EB 01?? 4C4C 4A75
```

**Trivial.72**

**CEN:** A family of overwriting, 72-byte direct infectors containing the texts 'Be Afraid....' and (depending on the variant) '*.COM' or '*.EXE' or '*.*'. All infected files can be detected with the same template.

```
Trivial.72         B801 3DBA 9E00 CD21 93B4 40B1 48BA 0001 CD21 B43E CD21 B44F
```

**Trivial.76**

**CN:** An overwriting, 76-byte direct infector containing the texts '*.COM' and 'Baalberith'. It infects only the first COM file of the current directory.

```
Trivial.76         BA64 AAB8 C357 81F2 FAAA 4E2D C11A 4DCD 21F9 BAFF 2481 EAFF
```

**Trivial.85.A**

**CN:** An overwriting, 85-byte direct infector containing the texts '*.cOm' and 'Anton Szandor LaVey'. It infects only the first COM file of the current directory.

```
Trivial.85.A       B824 BF4E BA4E 37F8 81F2 D037 3526 82FC CD21 BA3F 9481 F23F
```

**Trivial.85.B**

**CN:** An overwriting, 85-byte direct infector containing the texts 'Kazgaroth', '*.COM' and 'DarkWell'. It infects only the first COM file of the current directory.

```
Trivial.85.B       0F01 4FBA 4244 F535 0D3C 81EA A443 90CD 21F8 BA07 E48B D881
```

**Trivial.88**

**CN:** An overwriting, 88-byte direct infector containing the texts '*.COM' and 'Ride the wings of death!'. It infects only the first COM file of the current directory.

```
Trivial.88         BA4E EFB8 2517 FC05 DD25 81F2 D0EF CD21 BA31 6781 EA31 6693
```

**Trivial.97**

**CN:** An overwriting, 88-byte direct infector containing the texts '*.COm' and 'Borys; the Dragon of Dark Sun'. It infects only the first COM file of the current directory.

```
Trivial.97         BA56 C545 B8E0 26F8 81F2 C8C5 35E2 1BCD 21F5 BA1B BC8B D8F5
```

**Trivial.113**

**CN:** An overwriting, 113-byte direct infector containing the texts '*.COM' and 'Domine Satanas, Rex inferus, adoramus te!'. It infects only the first COM file of the current directory.

```
Trivial.113        BA4F 17B4 0181 EA0D 1680 F44F 4FCD 214E B8F3 11FC BA75 2247
```

**Trivial.173**

**CN:** An overwriting, 173-byte direct infector containing the text: '*.COM'. The virus does not infect COMMAND.COM, nor any file less than 173 bytes long.

```
Trivial.173          7468 817C 1AAD 0072 61B8 003D 8D54 1ECD 2193 B43F B904 00BA
```

**VCC.334**

**CN:** An encrypted, appending, 334-byte direct infector containing the texts 'One must fall', 'Nuke_Man', 'I-EAS Virus Creation Centre v0.19a', '[OF]', '[NM]' and '[IE-VCC v0.19a]'. It disables VSAFE in memory and infects three files at a time. Infected files are marked with byte 43H ('C') at offset 03h.

```
VCC.334              B440 B94E 018D 9606 00CD 21E8 0500 B43E CD21 C38D B61F 00B9
```

**VCC.447**

**CEN:** An encrypted, appending, 447-byte direct infector containing the texts 'Someone is at the door', 'American Gothic Vir', and 'Thespian'. All infected files are marked with byte 43h ('C') located at offset 03h. As the virus tries to infect every program, it destroys files other than those with the extension COM.

```
VCC.447              B440 B9BF 018D 9606 00CD 21E8 0500 B43E CD21 C38D B620 00B9
```

**VCC.449**

**EN:** An encrypted, appending, 449-byte direct infector containing the texts 'DEBUGGING IS VERY ILLEGAL (NOT!)', 'Someone is at the door', 'American Gothic Vir', 'Thespian', 'I-EAS Virus Creation Centre v0.19a', '[AG]', '[Th]', and '[IE-VCC v0.19a]'. Infected files are marked with 43h ('C') at offset 03h.

```
VCC.449              B440 B9C1 018D 9606 00CD 21E8 0500 B43E CD21 C38D B620 00B9
```

**VCL.214**

**CER:** An overwriting, 214-byte virus containing the texts '[Krautfresser written by Spooky]', '1996 Austria', and '*.com'. All infected files have their date- and time-stamps set to 00-08-80 00:00:00.

```
VCL.214              B803 35CD 21B4 25BA 8C01 CD21 87D3 CD21 B8F2 F905 1000 BA35
```

**VCL.268**

**CEN:** An overwriting, 268-byte virus containing the texts '*.COM', '*.EXE', '[VCL_MUT]', and 'The Pleasure 15 VirusEver have the pleasure?By eMpIrE-X'. Though programmed not to infect COMMAND.COM, a bug means this file does become infected. Files less than 268 bytes long are not infected.

```
VCL.268              7205 E81B 0073 0CB4 4EBA 3701 CD21 7203 E80D 00C3 2A2E 434F
```

**VCL.289**

**CN:** An overwriting, 289-byte virus containing the texts '*.COM', '[VCL_MUT]', and 'The Pleasure 17 VirusEver have the pleasure?By eMpIrE-X'. The virus does not infect files less than 289 bytes long.

```
VCL.289              817C 1A21 0172 61B8 003D 8D54 1ECD 2193 B43F B904 00BA DB01
```

**VCL.313**

**CN:** An overwriting, 313-byte virus which contains the texts '*.COM', '[VCL_MUT]', and 'Monet 7 VirusBy eMpIrE-X'.

```
VCL.313              2193 B440 B939 01BA 0001 CD21 B801 578B 4C16 8B54 18CD 21B4
```

**VCL.314**

**CER:** An overwriting, 314-byte virus which contains the texts 'ReIncanation written by Spooky. Austria 1996' and 'Befehl oder Dateiname nicht gefunden.'. All infected files have their date- and time-stamps set to 00-00-80 00:00:00.

```
VCL.314              B899 99CD 2181 FB99 9974 03E9 0200 CD20 B821 35CD 212E 891E
```

**VCL.326.A**

**EN:** An overwriting, 326-byte direct infector containing the texts '*.EXE', '[VCL_MUT]', and 'The Pleasure 10 VirusEver have the pleasure?By eMpIrE-X'. It can be detected by the template for VCL.326.B.

**VCL.326.B**

**CN:** An overwriting, 326-byte direct infector containing the texts '*.COM', '[VCL_MUT]', and 'The Pleasure 18 VirusEver have the pleasure?By eMpIrE-X'.

```
VCL.326              7468 817C 1A46 0172 61B8 003D 8D54 1ECD 2193 B43F B904 00BA
```

**VCL.340**

**CEN:** An overwriting, 340-byte virus containing the texts '*.COM', '*.EXE', '[VCL_MUT]', and 'The Pleasure 14 VirusEver have the pleasure?By eMpIrE-X'. Files less than 340 bytes long are not infected.

```
VCL.340              817C 1A54 0172 61B8 003D 8D54 1ECD 2193 B43F B904 00BA 0E02
```

**VCL.350**

**CN:** An overwriting, 350-byte virus which contains the texts '*.COM', '[VCL_MUT]', and 'Monet 8 VirusBy eMpIrE-X'.

```
VCL.350              2193 B440 B95E 01BA 0001 CD21 B801 578B 4C16 8B54 18CD 21B4
```

**VCL.442.A**

**EN:** An overwriting, 442-byte direct infector containing the texts '*.EXE', '[VCL_MUT]', and 'The Pleasure 11 VirusEver have the pleasure?By eMpIrE-X'. It can be detected by the template for VCL.442.B.

**VCL.442.B**

**CN:** An overwriting, 442-byte direct infector containing the texts '*.COM', '[VCL_MUT]', and 'The Pleasure 20 VirusEver have the pleasure?By eMpIrE-X'.

```
VCL.442              B43B 8D56 BACD 21BA 6801 E869 0073 02EB DAB4 3B8D 9679 FFCD
```

**VCL.456**

**CEN:** An overwriting, 456-byte virus containing the texts '*.COM', '*.EXE', '[VCL_MUT]', and 'The Pleasure 16 VirusEver have the pleasure?By eMpIrE-X'. Files less than 456 bytes long are not infected.

```
VCL.456              B43B 8D56 BACD 21BA 7001 E877 0073 0ABA 7601 E86F 0073 02EB
```

**YCTC.1729**

**CER:** A stealth, appending, 1729-byte virus containing the texts 'COMMAND', 'IBM', 'ET', 'PC', 'TB', 'CKVI', 'KLVI', 'DEVI', 'BTOOL', 'RTOOL', 'TDISK', 'SCAN', 'CLEAN', 'HUNT', 'F-', and 'You have a Y.C.T.C.Virus... Ha! Ha! Ha! Ha! == Written by Y.C.T.C.student 1995. == === I am y.c.t.c. student written... ==='.

```
YCTC.1729            E869 0056 B9C1 0690 33FF 8EC0 FCF3 A45E 07A1 0000 061F 3DCD
```

**Zyklon.754**

**CER:** An appending, 754-byte virus. When the virus is active in memory, Int 21h function 5454h returns the value AX=5400h and Carry Flag set ('Are you there?' call).

```
Zyklon.754           1E06 B854 54F8 CD21 726E B452 CD21 FA26 8E5F FE80 3E00 005A
```

FEATURE

# The Word of the Day

As discussed in last month's editorial (see *VB*, February 1997, p.2), *Microsoft* has just released a new version of its phenomenally huge and similarly successful *Office* suite, imaginatively entitled *Office 97*.

One of the major changes in the new versions of the constituent applications – apart from the fact that the word 'Internet' abounds – is the harmonisation of the most powerful automation component: the macro languages.

### A New Generation of Macros

*Microsoft* makes the point, and it is a legitimate one, that the new language is now too powerful to be referred to simply as a 'macro language'. All the *Office 97* applications use *VBA5* (*Visual Basic for Applications version 5*), which offers essentially the same functionality as the complete *Visual Basic version 5* – which should have shipped by the time you read this.

Clearly, therefore, as discussed last month, there must be an upgrade path for users with software written in *WordBasic* (as used in *Word 6.0* and *7.0*) and previous versions of *VBA* (as used in *Excel 7.0* and *Access 7.0*).

This is the first of two areas to be investigated in this article: how 'well' current *Word* macro viruses survive the transition to *Word 97*. It also examines the protections *Microsoft* has built into the new applications. The second part of the article looks at the opportunities for native *Word 97* viruses.

# Part One: Upgrade your viruses now!

For obvious reasons, the behaviour of *Word* macro viruses (those written for *Word 6.0* and *7.0*) is of great interest – these are, after all, the most commonly-reported type of virus in the world today.

### Initial Discoveries

It transpires that *Microsoft* has built into *Word 97* the ability to detect whether the document being loaded is infected with one of a limited series of *WordBasic* macro viruses. These viruses are *silently* removed from documents as they are loaded into the new version of *Word* – that is, the user is not told his document was ever infected; it is simply cleaned for him. This article does not intend to investigate the positive and negative aspects of this behaviour: suffice it for the moment to say that this is how it behaves.

However (and here's where the real fun begins), the viruses of which *Word 97* has specific knowledge are not listed anywhere in the on-line documentation, nor on *Microsoft's* Internet site. The author is grateful to Jimmy Kuo of *McAfee Associates* for providing a remarkably complete list of those viruses which make it through the conversion process, as well as those which are damaged or removed along the way.

This list is not reproduced here for reasons of space, but makes for curious reading – *Word 97* removes all or part of almost all variants of the more common, well-known macro viruses.

Concept, Wazzu, MDMA, NOP, Bandung, and NPad are all strongly represented in the 'damaged in conversion' list, along with other, less common, viruses. Notably, not all variants of most of those mentioned above were damaged, though only a very few more obscure variants made it through intact.

This fact alone, as mentioned in last month's editorial, will seriously restrict the spread of macro viruses. As more and more people move over to *Office 97*, many old-style macro viruses will be eliminated by this functionality.

### What Next?

Once a macro virus has been converted to *VBA5*, the next point to consider is whether the virus can work. In theory, if the conversion process is foolproof, all converted viruses would work. In practice, things are not that straightforward.

*Word 97* places more obstacles in the path of macro viruses. Just like *Word 7.0a*, it includes a feature called 'Macro virus protection'. This option (which is turned on by default), checks documents as *Word* opens them, and flags the user if a document 'contains macros or customisations' (see Figure 1).

The default option in the dialog is to load the document but disable the customisations – this means that if the document does indeed contain a virus, it is not present in the loaded copy, and will therefore be removed as soon as the document is resaved from *Word*.

The downside of this approach is that, if the document contains non-viral macros, they will also produce the alert, and be removed in the same way. In order to lessen the impact of this, there is a single special case (of which the author is aware!) – if the file is being loaded from the Templates directory (which, on a default installation, is to be found underneath C:\Program Files\Microsoft Office), the warning is not given.

There are several disadvantages to the warning. First, any user who often uses macros will probably disable the warning – it does become extremely annoying after a while! The opportunity to disable the warning is given on the

dialog itself (see Figure 1); it is not even necessary to go grubbing around in the Options dialog to locate the correct tick box.

There are also other problems. The document containing this article, for example, causes the dialog to be displayed every time it is opened, despite the fact that it contains no obvious macros or customisations.

Even more peculiar, if 'Disable Macros' is selected from the dialog, and the document is then re-saved under a different name, that new document also generates the alert! Clearly there are problems with this feature.

### Evolution

The future seems bleak, therefore, for *WordBasic* viruses. However, life is never that simple: indeed, already we have seen two perfectly normal *WordBasic* viruses, NiceDay.A and Wazzu.A, make the jump to *Word 97*. These instances illustrate two important points.

First, NiceDay.A is not spotted by the virus removal component of *Word 97*, although it will be noticed by the virus prevention component (if the user has this turned on). Therefore, the automatic creation of this *Word 97* version of the virus is not a surprise; it was only a matter of time.

The second, Wazzu.A, is more of a mystery. *Word 97's* virus removal component silently removes this particular virus as soon as an infected document is loaded, so how was it converted? Thereby, as they say, hangs a story.

### A Tale of One Web Site

In early February, a file was found on *Microsoft's* World Wide Web site. The file, REVCODES.EXE, was a self-extracting executable which unpacked to produce a *Word* document called WORD97~1.DOC. It was this file which contained a *Word 97* conversion of Wazzu.A. But how is this possible?

The answer is that it isn't. At least, it's not possible using the *release* version of *Office 97*. Unfortunately, all the pre-release and beta versions of the product did not include the virus removal component, and these pre-releases were distributed fairly widely, as part of the bid to encourage people to move up to *Office 97*.

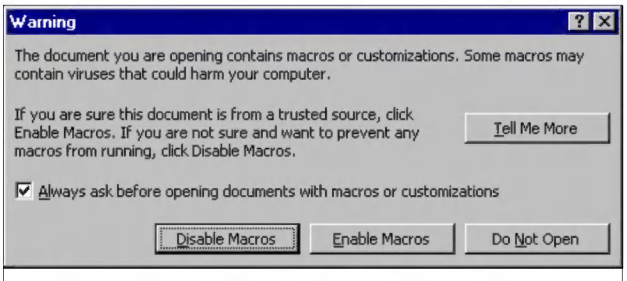



**Figure 1:** The dialog box displayed by *Word 97* when a document which may be infected is opened.

Consequently, any currently-existing macro virus can be converted by any pre-release version of the product, and from there move quite happily onto release versions. Of course, the 'macro virus protection' warning dialog will be produced, but if the user chooses the wrong option, or has turned this off…

The new virus – for a new virus it is, despite the fact that it is a conversion of an old one – has been named W97M/Wazzu.A (similarly, the conversion of NiceDay.A is called W97M/NiceDay.A).

## Part Two: New viruses?

After all this talk of how the past will convert, what of the chances for new viruses in the world of *Word 97*? There can be little argument with the belief that new viruses will be produced for the new environment: it seems absolutely inevitable. Having said that, there is, at least in the opinion of the author, a significant obstacle to their rapid production.

### Security through Obscurity?

*VBA5* is a much more difficult language to learn than *WordBasic*. It used to be fairly easy to bash together a working macro in relatively little time; this is no longer the case. This shallower learning curve is almost always the price to pay as the power and flexibility increase; increased power begets increased complexity.

Part of the reason for *VBA5's* complexity is its plentiful use of object-orientation – *VBA5* offers this in abundance. No longer does the programmer simply execute the 'Bold' command having selected a piece of text (as he did in *WordBasic*); now he takes the 'Font' property of the 'Selection' object, and toggles the setting of the 'Bold' property on that to 'True'. [*Obvious, really. Ed.*]

Despite this, it would be folly to believe that this will delay the production of new viruses for very long. It would be foolhardy to make a guess as to how long it will take for the first macro virus specifically written for *Word* (or indeed *Office*) *97* to appear – there are simply too many imponderables. Only one thing is certain – it will happen.

### Conclusion

Overall, it would seem that in the short term the inevitable gradual phasing in of *Office 97*, and the corresponding phasing out of *Office 95*, will serve to reduce the macro virus problem, due to both the virus removal and virus prevention components of the new *Word*.

But inevitably, old viruses will make the jump, and new ones will be created. It is for these reasons that anti-virus vendors are working flat out to deal with new file and macro formats. In fact, some developers have already announced versions of their products incorporating built-in detection (and, in some cases, removal) capabilities. *Office 97* users should certainly not consider themselves immune from the macro virus issue.

# VIRUS ANALYSIS

## On the Road to Mega-partism

Eugene Kaspersky

Like their biological counterparts, PC viruses evolve, taking on new forms and features, propagating to new platforms and occupying 'empty cells' in their computer universe. The most complex infectors are not satisfied with a single place to live, and occupy several. Such viruses, called 'multi-partite', infect more than just DOS files or disk sectors.

There are several types: those that infect DOS executable files (including SYS drivers) and boot sector infectors (this group is large; perhaps the best-known are Flip, Natas and One_Half), DOS and *Windows* files (for example, PH33R), and even DOS batch files and disk sectors (e.g. BLAH).

In late 1996 a new type of multi-partite virus appeared, infecting boot sectors as well as both DOS and *Windows* executable files… the first step from bi-partite to tri-partite viruses. Now, I'm waiting to see a mega-partite virus that infects all types of DOS, *Windows*, *Windows 95* executable files, disk boot sectors, *MS Word* documents, and *Excel* sheets. Anything is possible.

### Brief Guide

In its 3783 bytes of code, TPVO uses over 30 precisely-written subroutines, enabling it to support infection of all three target objects, as well as maintaining its complex stealth routines.

Individual infection methods are fairly standard. When infecting DOS COM and EXE files, TPVO writes itself to the end of the file and modifies the file's entry point in the file header. When infecting a NewEXE (NE) file, it also writes itself to the end of the file, but modifies the NE file header, creating a new Segment Table, fixing up other fields in the NewEXE header, and creating a new code segment to contain the virus code. When infecting a sector, the virus overwrites it with a short loader and saves its complete code to hidden disk sectors.

The virus does not manifest itself in any way and contains no text-string by which to name it. It is known by two names: TPVO, because it bears similarities to TPVO.3464, written by Dark Slayer of the 'Taiwan Power Virus Organization', and DS, after text-like data used in the virus' 'Are you there?' call (Dark Slayer's initials).

### Installation: DOS and Windows Executable Files

When an infected COM, EXE or NewEXE file is executed, the virus takes control and immediately runs its installation routine. First, it checks whether it is already present in system memory by using an 'Are you there?' call (Int 21h; AX=187Fh and BX=4453h ['DS']). If BX=87A1h is returned (indicating a resident copy), the virus returns control to the host program. Otherwise it walks the list of Memory Control Blocks and decreases the size of last block in order to reserve memory for its TSR copy.

Then the virus copies itself into this space, hooks Int 2Ah and returns to the host program. If the host is a DOS executable, TPVO parses the MCBs in both conventional and upper memory (if the latter exists). In the case of NewEXE files, the virus manipulates system memory with DPMI calls.

TPVO completes installation when Int 2Ah is next called. It then hooks Ints 13h, 21h, and 2Fh, and releases Int 2Ah. To hook Int 21h and Int 2Fh, the virus scans the DOS kernel for a certain specific piece of code, which it patches with FAR CALLs to its own Int 21h and Int 2Fh handlers.

The virus hooks Int 13h with an undocumented Int 2Fh call that is often seen in viruses: Int 2Fh, AH=13h. This enables TPVO to get the original Int 13h address, and to set the Int 13h address in the DOS kernel to a new value. Thus, it does not hook Int 13h directly, but writes a new value to the address used by the DOS kernel.

Further, the virus puts an address into the DOS kernel which does not point directly to the virus code, but to an area in system memory containing the JMP VIRUS instruction. Thus, the Int 13h handler receives control from the DOS kernel in two jumps: kernel to some-code, some-code to handler.

Depending on system conditions, the virus uses one of two methods to do this: it may look within the BIOS segment (F000h) for an Int XXh call (CDh XXh, where 7Fh < XXh < E0h) and then hook Int XXh and set the DOS kernel Int 13h address to the address of the CDh XXh code; or it may write a FAR JMP Virus_INT_13 command to the BIOS data area (at address 0000:04FBh) and set the Int 13h vector there.

### Installation: MBR or Diskette Boot Sector

When loading from an infected MBR, the virus loader reads its body (eight sectors) from disk to system memory at address 7C00:0000h and passes control there. Then it hooks Int 13h, using the Int XXh method described above.

To return control to the original MBR or floppy disk boot sector, the virus calls the Bootstrap loader (via Int 19h). When the system then accesses the boot sector, the virus' stealth routines are in place, which redirect the call to the original sectors. Thus, the boot process continues unimpeded.

When the system calls Int 13h, TPVO's handler takes control and checks the system. If DOS loading is complete, the virus hooks Int 2Ah and, on the first Int 2Ah call, hooks Int 21h and Int 2Fh as described above.

On the first execution of any program (Int 21h, AH=4Bh), the virus completes its installation routine: it patches the Memory Control Blocks, cuts a block of system memory (conventional or upper) and copies itself there.

### INT 13h Handler

The virus uses its Int 13h hook to complete the installation routine, to realize its stealth routine while reading from and writing to infected sectors, and to infect the MBR of the hard drive and the boot sector of floppy disks.

While infecting a disk sector, the virus overwrites it with 1Ch bytes of virus loader which reads the virus body at boot-time. Then the virus saves the original sector, in addition to its complete code, in the eight sectors, starting from the fifth on track 0, head 0 on the hard drive. In case of a diskette, the virus formats an extra track (the 80th) and writes the data there.

The virus realizes a 'lite' stealth routine that just redirects read/write calls (Int 13h, AH=2,3) to the sector containing the original boot sector or MBR. The virus does not hide the sectors that contain complete virus code.

### Int 21h Handler

The virus' Int 21h handler intercepts over ten DOS functions for its stealth and infection routines. When an infected file is accessed by any of the FindFirst/Next FCB/ASCII calls, the SeekEnd call, or the Get/Set Date&Time Stamp calls, the virus 'decreases' the apparent file length and restores the date/time field to its pre-infection value.

While writing (AH=40h) to an infected file, TPVO disinfects it. When the system reads from an infected file (AH=3Fh), the virus performs a complex stealth routine that restores the read buffer to its uninfected form. This happens for COM, EXE and NewEXE files. This is the first virus I have encountered to perform such a stealth routine while accessing NewEXE files.

When an infected file is accessed by any of the functions listed above, the virus compares the name of the active program with the list:

```
PKZIP ARJ RAR LHA TELIX BACKUP MSBACKUP CHKDSK
```

If there is a match, TPVO disables its stealth routines; thus, it stays invisible under any other environment. However, if an infected file is moved to an archive or backup, or is transmitted by Telix, the virus does not remove itself from the copied data.

When an executable file is closed, renamed, executed, loaded as overlay or for debugging, or accessed by the calls Get/Set FileAttributes (AH=3Eh, 43h, 56h, 4B0Xh), the virus infects it. To separate executable and data files, TPVO checks both the extension of the file's name, and its internal format, infecting the file if the filename extension is COM, or if its header contains the EXE stamp MZ.

While infecting a file, the virus uses undocumented System File Tables, Int 2Fh calls, and other tricks. It pays careful attention to the file attributes and date-stamp, and temporarily hooks Int 24h to disable the standard DOS error message while attempting to write to write-protected disks.

### Int 2Fh

Hooking Int 2Fh allows the virus to disable the undocumented Int 2Fh call GetAddressOfSystemFileTable (AX=1216h). The only reason I can see for this is to terminate direct access to file data and disable anti-stealth routines in anti-virus scanners.

## TPVO

Aliases: DS, DS.3783, TPVO.3783.

Type: Memory-resident multi-partite COM, EXE and NewEXE (Windows 3.x) files, Boot and MBR sectors infector. Stealth, but not encrypted.

Self-recognition in COM, EXE and NewEXE Files:
Adds 100 years to the year field in the file time- and date-stamp.

Self-recognition in Boot Sector and MBR:
Compares the word at offset 0046h with the word C48Eh.

Self-recognition in Memory (installing from an infected file):
'Are you there?' calls Int 21h, AX=187Fh and BX=4453h ('DS'). Memory-resident copy returns BX=87A1h.

Self-recognition in Memory (installing from an infected sector):
Does not check the system. TPVO's stealth routine does not allow infected sectors to be loaded into memory twice.

Hex Pattern in Files and Memory:

```
0E1F E800 005E 83EE 0556 06B8
7F18 BB53 44CD 2181 FBA1 8775
3A07 5E0E 1F8B 8487
```

Hex Pattern in Sectors:

```
FA33 DB8E D3BC 007C 8EC4 B808
02B9 ???? BA?? ??CD 1372 0006
68C3 00CB ???? ????
```

Intercepts: Int 2Ah on installing TSR copy, Ints 13h, 21h, and 2Fh for infection and stealth.

Trigger: None.

Removal: Under clean system conditions, identify and replace infected files. To recover an infected MBR, use FDISK /MBR; to clean boot sectors on floppy disks, use the SYS command.

# COMPARATIVE REVIEW

## Serving the World

Once again, the *NetWare* comparative circus rolls into town: this time, thirteen products submitted themselves for a head-to-head comparison.

One of the problems in performing a review of this kind is to ensure all products are assessed according to the same criteria – not always easy, as not all products will have implemented a particular feature in an identical, or indeed a similar, manner.

There are also myriad definitions for the various facilities available. In this review, 'on-demand' (or 'immediate') scanning is defined as the scanner being requested to carry out a scan of selected areas straight away. Real-time (on-access) scanning is when the scanner checks files as they are accessed; e.g. file in, file out, rename, move. Scheduled scanning is viewed as running or repeating a scan at a pre-defined time or interval of time.

The main purpose of these tests is to check the basic functionality of the products in certain critical areas; namely, detection rates and server overhead. The detection tests are based on the usual *Virus Bulletin* test-sets – In the Wild, Standard and Polymorphic.

The In the Wild set, based on the October 1996 WildList, reflects those viruses found in the real world. The Standard test-set includes a selection of various viruses to see how well different scan engines can handle different virus mechanisms, and the Polymorphic test reviews how well the scan engines cope with viruses which change their appearance radically from file to file.

Assessing the server overhead for on-access checking determines what extra delay can be expected when running such a scan. There is little practical benefit to be gained from having a scanner with a high detection rate, if its usage inconveniences users significantly by imposing a large delay.

Under each product, the default file extensions used by the scanner are listed: this indicates which file types will be scanned by default. It is important to realise that some scanners do not automatically scan for macro viruses if their file extension lists are not augmented to include the required file extensions, even though the scanner has the technology to recognise the various virus signatures.

Having done that, the comparison considers and compares what other features are on offer to the *NetWare* administrator. The various facilities can be split, essentially, into two categories: scanner configuration options and general administration (including installation).

### Scanner Configurations

This covers scanner options such as Immediate (on-demand), Scheduled (timed) and On-access (real-time) – in each case the amount of control is considered. For an immediate scan, does the user have Start/Stop control? For a scheduled scan, what scan frequency options are available? For an on-access scan, can Incoming/Outgoing checks be selected?

The configurability of file types and areas of the server to be scanned are noted. When a virus is detected, what options are available to manage and report the infection? Separately, the options available to alert users and supervisors are considered.

### Administration and On-access Scanning

Administration deals with installing, managing, and updating the product. There is a growing trend towards supplying products on CD-ROM, though 3.5-inch floppies predominate.

To handle scanner configuration, some programs can be managed either from the workstation or the server console. Finally, in this area, consideration is given to how signature updates are managed, and what other facilities are available.

On-access scanning is an accepted facility to provide immediate detection of viruses before the file can be accessed. The amount of real-time or on-access overhead varies between products. The usual compromise between the level of protection and performance is to scan incoming files only. If, for whatever reason, this is insufficient protection, both incoming and outgoing scans can be carried out.

### Virus Management

There is, as ever, a difference of opinion regarding disinfection. Many products do not provide the facility, relying on complete removal of the problem. Aside from disinfection, there are plenty of methods to handle viruses on detection – move, delete, rename, and copy are all provided by most products.

Most of the products deal with an infected file as soon as it is detected. However, some wait until the scan is completed before tackling each one, sometimes individually. This is fine for a couple of infections, but could be a major problem if several hundred files became infected.

### Cheyenne InocuLAN v4.0/3.23

In the Wild: 88.4% Standard: 97.1% Polymorphic: 91.1%
NetWare Versions supported: 3.1x, 4.x
Default File Extensions (Windows workstations): APP DRV EXE OVL OVR PRG SYS
Default File Extensions (Server & DOS): APP COM DRV EXE OVL OVR PRG SYS

| | In the Wild | | Standard | | Polymorphic | |
|---|---|---|---|---|---|---|
| | Number | Percent | Number | Percent | Number | Percent |
| Cheyenne InocuLAN | 404 | 88.4% | 508 | 97.1% | 10354 | 91.1% |
| Command F-PROT | 444 | 94.8% | 532 | 100.0% | 11000 | 100.0% |
| CYBEC VET_NET | 469 | 98.5% | 518 | 98.4% | 11000 | 100.0% |
| Dr Solomon's AVTK | 469 | 99.4% | 530 | 99.6% | 10997 | 98.8% |
| EliaShim ViruSafe | 462 | 98.8% | 435 | 89.3% | 9439 | 78.0% |
| ESaSS ThunderBYTE | 464 | 97.5% | 532 | 100.0% | 10841 | 95.5% |
| H+BEDV AVNet | 431 | 91.0% | 486 | 94.8% | 8394 | 73.1% |
| IBM AntiVirus | 470 | 99.4% | 531 | 99.6% | 10998 | 97.7% |
| Intel LANDesk Virus Protect | 472 | 99.1% | 359 | 79.0% | 10366 | 91.1% |
| Norman Firebreak | 470 | 99.3% | 532 | 100.0% | 11000 | 100.0% |
| Sophos SWEEP | 467 | 99.3% | 526 | 99.2% | 11000 | 100.0% |
| Symantec Norton AntiVirus | 461 | 98.1% | 453 | 91.2% | 6734 | 60.7% |
| Trend ServerProtect | 468 | 98.7% | 359 | 79.0% | 10366 | 91.1% |

*Cheyenne's InocuLAN* is designed to interface with its *ArcServe* range of backup products, and the Domain Manager provides the supervisor with a centralized overview of the network.

Selecting a particular server allows the status of the various jobs running or waiting to be monitored. With this in mind, when a scan is running, a bar is displayed which keeps track of the progress of a scan – this is useful for server scanning, as the supervisor can estimate time until completion more easily.

The DOS version of the administration program is able to shell out to DOS. When used with the workstation components, an extra measure of security can be added using Enforcement, which checks whether a user has IMMUNE (the memory-resident workstation component) loaded when they log in. If not, the user is given a grace period to load the software or be disconnected.

There are one or two inconsistencies: the list of file extensions is different from the DOS/Server list to the *Windows* list (bizarrely, COM is missing from the *Windows* list!), and, whereas page two of the help documentation refers to 'Immediate Scan', the program itself refers to 'Job Queue Operation'.

## Command Software F-PROT v2.24c

In the Wild: 94.8% Standard: 100.0% Polymorphic: 100.0%
NetWare Versions supported: 3.1x, 4.x
Default File Extensions: COM DO? DRV EXE FON OV? PGM SYS XL?

*F-PROT* provides, in addition to the comprehensive options available from the console command line, an Administration program, which runs on a *Windows* workstation. Also included is *AlertTrack Lite*, from *Software Inc*, which provides powerful alert management features. *F-PROT* can operate in a multi-server domain, where the different servers synchronise with a primary server so as to use the same scan and report settings.

*AlertTrack Lite* provides external communications options, including access to *Pegasus Mail*. Should a problem occur, another utility, TTCONFIG.NLM, is supplied: this collects information on the current *NetWare* environment (e.g. any modules loaded). This utility only runs with *F-PROT*.

## CYBEC VET_NET v9.22/29.11.96

In the Wild: 98.5% Standard: 98.4% Polymorphic: 100.0%
NetWare Versions supported: 3.x, 4.x
Default File Extensions: BIN COM DLL DO? EXE OV? PIF SYS

With this product, all scanner control and configuration is performed from the console. So-called 'Configuration Sets' are created, which cover scan modes and password protection. If necessary, scheduled configurations can be marked as 'disabled' for later use. Up to sixteen different configuration sets can exist simultaneously. The scanner has two levels of detection: 'Intelligent', which examines those areas of a file likely to be harbouring an infection, and 'Blind', which checks a file byte by byte.

The initial copy of the product had a bug in the code to move infected files to a quarantine area. A new version was promptly supplied, which fixed the glitch.

## Dr Solomon's AVTK v7.65/23 Oct 96

In the Wild: 99.4% Standard: 99.6% Polymorphic: 98.8%
NetWare Versions supported: 3.x, 4.x
Default File Extensions: APP BAT BIN CMD COM DEV DLL DOC DOT EXE OV? QLB SYS XTP 001 002

| | Cheyenne InocuLAN | Command F-PROT | CYBEC VET_NET | Dr Solomon's AVTK | EliaShim ViruSafe | ESaSS T'BYTE | H+BEDV AVNet | IBM AntiVirus | Intel LANDesk | Norman Firebreak | Sophos SWEEP | Symantec Norton AntiVirus | Trend Server Protect |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Installation** | | | | | | | | | | | | | |
| Supplied Media | CD-ROM | 3.5-inch | 3.5-inch | 3.5-inch | 3.5-inch | 3.5-inch | 3.5-inch | CD-ROM | CD-ROM | 3.5-inch | 3.5-inch | 3.5-inch | CD-ROM |
| Selectable Target Directory | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Forced Scan on Completion | | | | | | | | | | | | | |
| Option to Update AUTOEXEC.NCF | | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Option to Update Workstation Files | ✓ | | | | | | | | ✓ | | | | ✓ |
| **Administration** | | | | | | | | | | | | | |
| Password-protected Admin | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Password-protected Unload | | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | | ✓ |
| Windows Client Admin Tool | ✓ | ✓ | | ✓ | ✓ | | | | ✓ | | | ✓ | ✓ |
| DOS Client Admin Tool | ✓ | | | | ✓ | | | ✓ | | | | | |
| Admin from Server Console | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Server Grouping (Domains) | ✓ | ✓ | | | ✓ | Partial | | | ✓ | Partial | | ✓ | ✓ |
| Multi-server Admin Management | ✓ | ✓ | | | ✓ | | | | ✓ | | | ✓ | ✓ |
| **Signature Updates** | | | | | | | | | | | | | |
| **Network Updating** | | | | | | | | | | | | | |
| Server-to-server Updates | ✓ | ✓ | | | | | | | ✓ | | | ✓ | ✓ |
| Automatic Workstation Update | ✓ | ✓ | | ✓ | ✓ | | | | ✓ | | InterCheck | | ✓ |
| **Sources – Automatic** | | | | | | | | | | | | | |
| BBS | ✓ | | | | | | | | ✓ | | | | |
| Internet | | | | | | | | | ✓ | | | | ✓ |
| **Sources – Manual** | | | | | | | | | | | | | |
| Mail (floppy disk) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| BBS | ✓ | ✓ | | ? | ✓ | | | | ✓ | | ✓ | ✓ | ✓ |
| Internet Service | ✓ | ✓ | | ? | ✓ | | | ✓ | ✓ | | ✓ | ✓ | ✓ |

*Dr Solomon's AntiVirus Toolkit for NetWare* now offers a *Windows* utility for configuring the server, which neatly displays the command-line options to pass to the NLM in order to start it with the chosen options. As the supervisor becomes more familiar with the product, these options can be given directly by loading the respective NLMs with the requisite parameters.

As soon as the product is loaded, an immediate scan is started; all such scans can only be stopped by making use of an undocumented feature. Users should be made aware of this option, since a server scan is not a trivial activity, and may have been set in motion with incorrect settings.

There is much emphasis on the result codes which can be obtained from the different utilities. This provides the administrator with the opportunity to embed the scanner into a *NetWare* Command File (NCF) to provide additional processing as required.

## EliaShim ViruSafe v7.01/12-08-96

In the Wild: 98.8% Standard: 89.3% Polymorphic: 78.0%
NetWare Versions supported: 3.x, 4.x
Default File Extensions: COM EXE OV? SYS

The first version of *ViruSafe* submitted for review contained a bug – the scanner would always crash on certain (valid!) samples of Code.3952:VICE.05, requiring that the server be re-started. After a slight delay, a new version of the product was provided which fixed the problem.

The product works by creating jobs which are submitted for execution as required. It also uses a feature called InterServer as opposed to in-built real-time detection. For external communication, *ViruSafe* writes alert messages to its log files, which can be read by *AlertTrack* and forwarded via any selected communication medium. *AlertTrack* is, however, an additional cost item.

The real-time scan had to be changed since there is no real-time checking on the server itself; InterServer is used to check files accessed by the clients.

When creating a job under the *Windows* administration, if the user list was displayed more than once, the entries in the list were doubled. The whole list is added again up to the limit of 64 users. This 'feature' was found in the previous review copy (see *VB*, November 1996, p.22).

The extensions DO? and XL? had to be added to the Files List to check the In the Wild list. These additions are not retained in the default list when the NLM Job Console program is closed, only in those jobs already created.

## ESaSS ThunderBYTE v1.53c/10 Oct 1996

In the Wild: 97.5% Standard: 100.0% Polymorphic: 95.5%
NetWare Versions supported: 3.x 4.x
Default File Extensions: APP BAT BIN COM DLL DOC DOT DRV EXE OVL OVR SYS XLS XLM XLC XTP VBX 386

| | Cheyenne InocuLAN | Command F-PROT | CYBEC VET_NET | Dr Solomon's AVTK | EliaShim ViruSafe | ESaSS T'BYTE | H+BEDV AVNet | IBM AntiVirus | Intel LANDesk | Norman Firebreak | Sophos SWEEP | Symantec Norton AntiVirus | Trend Server Protect |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Scanner Options** | | | | | | | | | | | | | |
| **Immediate Scan** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Start/Stop User Control | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Scheduled Scan** | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Frequency: Once | ✓ | | | | ✓ | | ✓ | ✓ | | | | ✓ | |
| Now | | | | | ✓ | | | | | | | | |
| Hourly | ✓ | | | ✓ | ✓ | | | | | | ✓ | ✓ | |
| Daily | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Weekly | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| Weekdays | ✓ | | | | | | | ✓ | | | ✓ | ✓ | |
| Monthly | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | | | ✓ | ✓ |
| Quarterly | | ✓ | | | | | | | | | | | |
| Yearly | | | | ✓ | | | | | | | | | |
| Repeat | ✓ | ✓ | | ✓ | | | ✓ | ✓ | | | ✓ | | |
| **Scheduled Options** | | | | | | | | | | | | | |
| Run Program after Scan | | | | ✓ | | | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| Handle Concurrent Schedules | | ✓ | | ✓ | | | ✓ | ✓ | | | | ✓ | |
| **On-access (Real-time) Scan** | ✓ | ✓ | ✓ | ✓ | InterServer | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Configurable In/Out Control | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Command-Line Load Options | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | |
| Control CPU Usage | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | | |
| **Area Selection** | | | | | | | | | | | | | |
| File Extensions User Modifiable | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Directory/File Selection | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Directory/File Exclusion | | ✓ | ✓ | | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| **Virus Management** | | | | | | | | | | | | | |
| Report Only | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Delete | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Securely Delete/Purge | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | |
| Disinfect | ✓ | ✓ | | ✓ | ✓ | | | ✓ | ✓ | | Macros Only | | ✓ |
| Rename | ✓ | ✓ | ✓ | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Quarantine/Move | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Disconnect Workstation | ✓ | ✓ | | ✓ | | | ✓ | | | | InterCheck | ✓ | |
| Deny Access to File | | ✓ | | ✓ | ✓ | | | ✓ | | | | ✓ | |
| **Alert Management** | | | | | | | | | | | | | |
| Alert Supervisor | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Alert Selected Group | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Alert Workstation | ✓ | | | ✓ | | | ✓ | ✓ | ✓ | ✓ | InterCheck | ✓ | |
| Audible Alert | ✓ | | | ✓ | | | ✓ | | ✓ | | | | ✓ |
| Fax | ✓ | AlertTrack | | | | | | | | | | | |
| Pager | ✓ | AlertTrack | | | | | | | | | | ✓ | |
| Email MHS | ✓ | AlertTrack | | | | | ✓ | ✓ | | | | ✓ | |
| SNMP | ✓ | AlertTrack | | | | | | | ✓ | | | | ✓ |

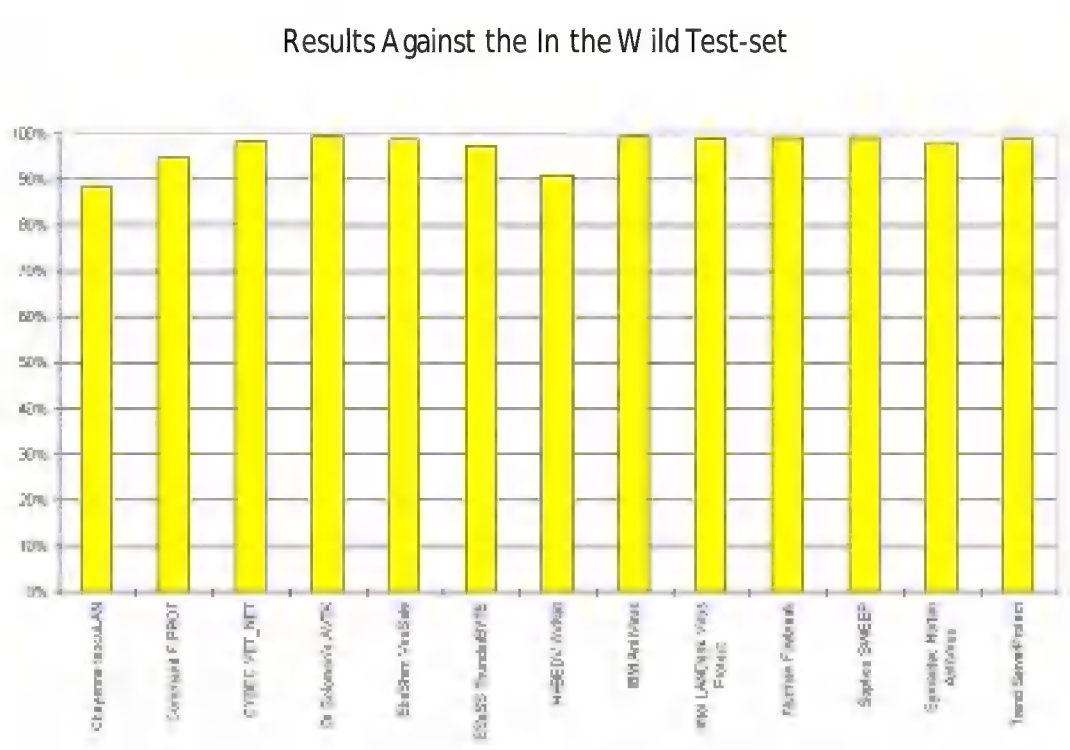
Many of the comments which are made about *Norman Data Defense's Firebreak* (see p.15) apply here: it appears to be the same engine, even down to the reference to the non-existent 'Schedule' option. The main difference appears to be in the virus signature list; the minor variations in the server overhead timings are within error.

The product provides limited inter-server communication features; it allows one server to be configured as a communication hub. Any other servers can be enabled to send alert messages to this hub.

## H+BEDV AVNet v1.02/10.12.1996

In the Wild: 91.0% Standard: 94.8% Polymorphic: 73.1%
NetWare Versions supported: 3.x, 4.x (Bindery Mode)
Default File Extensions: APP BIN COM DLL DOC DOT EXE OVR OV1 OV2 OVL PGM SMM SYS XTP

This is a console-based product which has the three usual scan modes, in addition to a separate CRC (Cyclic Redundancy Check) facility. It can be configured to load NLMs




The virus management is not handled immediately on detection, but at the end of the scan – fine for a few viruses, but a major infection could be tedious to control. An evaluation option creates log files for files scanned and any viruses detected. Whilst notionally for product evaluation, this is a useful facility for an initial server scan. The initial scan can be lengthy, due to the creation of a CRC table; however, subsequent scans are much more rapid.

both before and after an immediate scan. An unusual feature in this product is its ability to prevent certain users from logging on!

*AVNet* has another useful facility, called NETINFO.NLM, which reports on various *NetWare* settings. There is a listing of the viruses known by the scanner, but this only shows the name: no descriptions are available.

## IBM AntiVirus v2.5.1b

In the Wild: 99.4% Standard: 99.6% Polymorphic: 97.7%
NetWare Versions supported: 3.1x, 4.x
Default File Extensions: BIN COM DOC DOT EXE OV? SYS SMM XL?

As usual, the detection figures from the *IBM* product are impressive; however, the user interface does seem very dated. Installation involves copying and unzipping various files – the instructions for installing the Administration software are in a separate manual. It does seem a pity that all of this cannot be made more user-friendly by wrapping it all in an installation program – it could save a lot of documentation.

The product is driven by command-line options given at the console. These option settings can also be stored in the profile file, which is easy to edit using a text editor; there are around twenty-eight options to be administered. The administration software makes the managing of these profile files more user-friendly by having a set of menus to handle these options, rather than a flat file.

Up to five different schedules can be configured, as well as a scan to be triggered after the server is started. There is even an option to repeat a scan every five minutes, for testing and demonstrations.

## Intel LANDesk Virus Protect v4.0/206

In the Wild: 99.1% Standard: 79.0% Polymorphic: 91.1%
NetWare Versions supported: 3.x, 4.x
Default File Extensions: BIN COM DSK EXE LAN NAM NLM OVL SYSVAPVIR

*Intel's* scanning engine is based on that of *Trend*; hence, some comments apply to both products, especially those in the area of virus detection. The main change is that the file extensions are different – this may be due to the difference in signature levels supplied for evaluation. However, *Intel* takes the basic engine and integrates it into its *LANDesk* product family.

External communication options are handled using *Intel's* own Alert Management System. Alert messages are issued when changes to configuration are made. This can be very useful to monitor activity on a remote server.

An additional feature is Integrity Shield, used to prevent users with Supervisor-equivalent access rights moving infected files into certain designated areas. *LANDesk* comes with a report writer utility which can take the log files from the scanner in CSV format and produce management reports. It is the only product tested which specifically supports *MS Mail*.

## Norman Firebreak v3.53d 25/11/96

In the Wild: 99.3% Standard: 100.0% Polymorphic: 100.0%
NetWare Versions supported: 3.11, 3.12, 4.xx
Default File Extensions: APP BIN COM DLL DRV EXE OVL OVR SYS VBX XTP 386 BAT DOC DOT XLS XLM XLC

*Firebreak* has a fixed set of file extensions – they are not user-modifiable. Specific file inclusion and exclusion is also not available – with this one, it's all or nothing. There is no scheduled scan option, although one is alluded to in the menu options along with the Immediate scan option.

The console interface is intuitive and easy to use. *Firebreak* can accept communication from its range of workstation products if a virus is detected, and supports use of a central communications hub. Updates will be available through BBS and the Internet from version 4.

## Sophos SWEEP v2.91

In the Wild: 99.3% Standard: 99.2% Polymorphic: 100.0%
NetWare Versions supported: 3.11, 3.12, 4.x
Default File Extensions: ADD BID COM DLL DMD DOT DRV EXE FLT I13 IFS MOD OV? SCR SYS TSD VSD VXD

*Sophos* does not offer a remote configuration utility; *SWEEP* is configured from the server console. The product, in addition to the standard immediate, scheduled, and on-access scans, has a utility called InterCheck, a resident program designed to run memory-resident on network clients that sends new unchecked files to the server for scanning. Once checked, a file's checksum is stored locally for future reference.

As *SWEEP* also offers on-access scanning at the server, and to make a valid performance comparison with other products, the InterCheck facility was not used in these tests.

## Symantec NAV v2.02/12NAV96A

In the Wild: 98.1% Standard: 91.2% Polymorphic: 60.7%
NetWare Versions supported: 3.11, 3.12, 4.x
Default File Extensions: APP BIN COM DLL DOC DOT EXE OV? PRG SYS VXD XTP 386

This product does not allow complete deselection of the real-time scan options. Either incoming or outgoing can be deselected, but not both at the same time. This means that the overhead tests were incomplete but only missed the check on the initial overhead of having the NLM loaded.

The console status information can be viewed remotely using the workstation administration program. This allows a remote administrator to monitor what is happening on the server. The report logs can be configured to include administration functions such as the virus signature update and loading/unloading the NLM as well as the standard virus alerts. These reports can be filtered with options to produce hard copy or to create a test file for separate analysis.

The Update program was unable to find the default directory holding the NLM, without the drive being selected (a:>12NAV96A.exe sys:system\navnlm /dump). Updated files are not activated until the NLM is unloaded and then reloaded, despite what is said in the notes (or is it that there is a time delay before the new set is activated, which is not documented anywhere?).

## Trend ServerProtect v3.0/2.26

In the Wild: 98.7% Standard: 79.0% Polymorphic: 91.1%
NetWare Versions supported: 3.x, 4.x
Default File Extensions: BIN COM DOC DOT EXE OVL SYS XLS

As mentioned previously, *Trend Micro Devices* provides the scanner engine for the *Intel's LANDesk Virus Protect*. Therefore, many of the comments relating to the scanning engine will apply to both products. However, there are some differences. For example, the default file extensions differ from those of *Intel*, and the signature list sent with the evaluation copy was more recent.

One problem was encountered with the initial load of the scanner NLM. Before this happened, PSCAN.NLM (which is a file system hook program from *Intel*) kept crashing. It appeared that the version shipped was version 1.09, which had a problem with the *Novell* library updates in the LIBUP9 pack. By using version 1.11 of PSCAN.NLM, shipped with *Intel's LANDesk Virus Protect*, the scanner worked without problems.

In view of publication deadlines, this configuration was used as the basis of the tests performed. This was deemed to be justified, since it worked (always a good reason!), and also because any new version from *Trend Micro Devices* would in any case have been derived from that of the *Intel* product. The awaited version from *Trend* arrived shortly after completion of testing.

The integrity shield is the same as that of the *Intel* product; protected extensions are COM, EXE, BIN, OVL, and SYS. The integrity shield is a way to prevent users deleting or modifying selected directories or files, which ensures that supervisor-equivalent users can be restricted from spreading viruses where supervisors only have modify rights. *Trend* also offers its own BBS download facility for virus signature updates.

### Summary

The products seem to group themselves based on functionality. The fundamental facility is virus detection: it is good to see that, overall, the detection rates are an improvement over the last comparison.

## Overhead Tests of On-access Scanning

| | NLM loaded | | |
|---|---|---|---|
| | Read: No Write: No | Read: Yes Write: No | Read: Yes Write: Yes |
| Cheyenne InocuLAN | 73.8% | 115.5% | 119.2% |
| Command F-PROT (AlertTrack) | 89.2% | 97.3% | 104.4% |
| Command F-PROT | 2.6% | 6.7% | 16.8% |
| Cybec VET_NET | 1.8% | 4.6% | 31.1% |
| Dr Solomon's AVTK | 80.6% | 88.5% | 100.4% |
| EliaShim ViruSafe | 7.4% | N/A | 122.9% |
| ESaSS ThunderBYTE | 97.4% | 106.6% | 114.7% |
| H+BEDV AVNet | 67.6% | 74.2% | 102.6% |
| IBM AntiVirus | 87.7% | 115.6% | 144.5% |
| Intel LANDesk Virus Protect | 86.6% | 239.0% | 274.2% |
| Norman Firebreak | 82.4% | 95.3% | 132.9% |
| Sophos SWEEP | 77.3% | 81.4% | 103.3% |
| Symantec Norton AntiVirus | N/A | 77.8% | 78.6% |
| Trend ServerProtect | 78.4% | 200.0% | 278.1% |

The default list of extensions to be scanned in each product varies considerably. However, in all but two cases (*ESaSS' ThunderBYTE* and *Norman's Firebreak*), the products allow additional file types to be added as necessary. Incidentally, the same two products are the only ones which do not provide a scheduled scan option.

The need to minimise the scanner's interference with normal server activity is well recognized, with many of the products providing a configuration option either to adjust the rate at which files are opened for scanning, or to set a threshold for CPU utilisation. Some take a dynamic approach, stating that they try to use CPU idle time to provide the necessary processing. As for selectability of files and directories, most products offer some ability to provide selectivity, but a few prefer an 'all-or-nothing' approach.

### Conclusion

The products which were evaluated provide the basic facility of virus detection in various forms, while also attempting to minimise the inevitable additional load this work brings to the server. Through a careful selection of on-access scanning, combined with a specific server scan prior to archiving, a network manager can feel fairly confident about providing protection without making the user access time unacceptable.

The biggest difference between the products is in the area of alert management and inter-server communication. This difference seems to be due to the markets either side of the Atlantic, with the US-based products providing for the most part a much higher level of multiple server management than products from Europe and elsewhere.

At one end of the scale, a number of the products simply provide single-server protection with control from the server. The other end sees products which provide protection for the server and have interaction with the scanners running on network-attached workstations. These may or may not have workstation administration as well as console control.

Products on the next level have the ability to manage multiple servers within a security domain. Finally, there are products which have automated signature updates from bulletin boards or from the Internet, and provide inter-server communication to give automated signature deployment to servers and workstation download.

The time when a user had to decide between reliable virus detection and functional multi-server management now seems to be passing: vendors are now providing both the functionality and effective scanners. This is not a trivial task. The skills necessary for virus detection and network communication are different, and some vendors have made a conscious decision to stick to their area of expertise, and to collaborate with other developers who have complementary products.

There is certainly a growing need for enterprise support for networked solutions providing *NT* and *NetWare* support, with automatic deployment of workstation updates from pre-programmed downloads using Internet-connected bulletin boards. One hopes that this scenario, in future, will relieve the network supervisor from the mundane task of maintaining up-to-date virus protection and minimise the risk to an organisation of a virus infection caused by out-of-date scanners failing to detect the latest crop of viruses.

**Hardware Used:**
Server – *Compaq Prolinea 590* with 16MB RAM and 2GB of hard disk.
Workstations – a selection of *Compaq* 386 and 486 machines.

**Software Used:**
Server – *NetWare 3.12*, with LIBUP9 applied.
Workstations – *MS-DOS* 6.22, *Windows 3.1*, *NetWare* VLMs v1.21.

**In the Wild Test-set. 476 samples of 134 viruses, made up of:**

Alfons.1344 (5), Anticad.4096.Mozart (4), Arianna.3375 (4), Avispa.D (2), Backformat.2000.A (1), Bad_Sectors.3428 (5), Barrotes.1310.A (2), BootEXE.451 (3), Burglar.1150.A (3), Byway.A (1), Byway.B (1), Cascade.1701.A (3), Cascade.1704.A (3), Cawber (3), Changsa.A (5), Chaos.1241 (6), Chill (1), Cordobes.3334 (3), CPW.1527 (4), Dark_Avenger.1800.A (3), Delta.1163 (6), DelWin.1759 (3), Desperado.1403.C (2), Die_Hard (2), Digi.3547 (5), Dir_II.A (1), DR&ET.1710 (3), Ear.Leonard.1207 (3), Fairz (6), Fichv.2_1 (3), Flip.2153 (2), Flip.2343 (6), Freddy_Krueger (3), Frodo.Frodo.A (4), Ginger.2774 (2), Goldbug (3), Green_Caterpillar.1575.A (3), Hare.7610 (2), Hare.7750 (8), Hare.7786 (9), Helloween.1376.A (6), Hi.460 (3), Hidenowt (6), HLLC.Even_Beeper.B (3), Istanbul.1349 (6), Jerusalem.1244 (6), Jerusalem.1500 (3), Jerusalem.1808.Standard (2), Jerusalem.Mummy.1364.A (3), Jerusalem.Sunday.A (2), Jerusalem.Zero_Time.Australian.A (3), Jos.1000 (3), June_12th.2660 (6), Junkie (1), Kaos4 (6), Karnivali.1971 (3), Keypress.1232.A (2), Lemming.2160 (5), Liberty.2857.A (2), Little_Red.1465 (2), Macgyver.2803 (3), Major.1644 (3), Maltese_Amoeba (3), Mange_Tout.1099 (4), Manzon (2), Markt.1533 (3), Mirea.1788 (2), Natas.4744 (5), Necros.1164 (2), Nightfall.4518.B (2), Nomenklatura.A (6), November_17th.800.A (2), November_17th.855.A (2), No_Frills.Dudley (2), No_Frills.No_Frills.843 (2), Npox.963.A (2), One_Half.3544 (5), One_Half.3570 (3), Ontario.1024 (3), Pathogen:SMEG.0_1 (5), Ph33r.1332 (5), Phx.965 (3), Pieck.4444 (3), Plagiarist.2051 (3), Predator.2448 (2), Quicky.1376 (1), Reverse.948 (3), Sarampo.1371 (6), Sat_Bug.Sat_Bug (2), Sayha (5), Screaming_Fist.II.696 (6), Sibylle (3), Sleep_Walker.1266 (3), SVC.3103.A (2), Tai-Pan.438 (3), Tai-Pan.666 (2), Tanpro.524 (6), Tentacle.10634 (4), Tentacle.1996 (3), Tequila.A (3), Teraz.2717 (5), Three_Tunes.1784 (6), Trakia.653 (3), Tremor.4000.A (6), Trojector.1463 (6), Trojector.1561 (3), TVPO.3873 (9), Unsnared.814 (3), Vacsina.TP-05.A (2), Vacsina.TP-16.A (1), Vampiro (2), Vienna.648.Reboot.A (3), Vinchuca (3), VLamix (3), Werewolf.1500.B (3), WM.Buero (4), WM.Colors.A (4), WM.Concept (4), WM.Date (4), WM.Divina (4), WM.Hot (4), WM.Imposter (4), WM.Irish (4), WM.MDMA (4), WM.NOP.A (4), WM.NPad (4), WM.Nuclear.B (4), WM.Wazzu (4), Xeram.1664 (4), XL.Laroux (4), Xuxa.1984 (6), Yankee_Doodle.TP-39 (5), Yankee_Doodle.TP-44.A (5), Yankee_Doodle.XPEH.4928 (2).

**Standard Test-set. 532 samples of 256 viruses, made up of:**

Abbas.5660 (5), Accept.3773 (5), AIDS (2), AIDS-II (1), Alabama (1), Alexe.1287 (2), Algerian.1400 (3), Amazon.500 (2), Ambulance (1), Amoeba (2), Anarchy.6503 (5), Andreew.932 (3), Angels.1571 (3), Annihilator.673 (2), Another_World.707 (3), Anston.1960 (5), Anthrax (1), Anti-Pascal (5), Anticad.4096.A (4), AntiGus.1570 (3), Argyle (1), Armagedon.1079.A (1), Assassin.4834 (3), Attention.A (1), Auspar.990 (3), Baba.356 (2), Backfont.905 (1), Barrotes.840 (3), Bebe.1004 (1), Big_Bang.346 (1), Billy.836 (3), BlackAdder.1015 (6), Black_Monday.1055 (2), Blood (1), Blue_Nine.925.A (3), Bosnia:TPE.1_4 (5), Burger (4), Burger.405.A (1), Butterfly.302.A (1), BW.Mayberry.499 (3), BW.Mayberry.604 (6), Cantando.857 (3), Cascade.1701.Jo-Jo.A (1), Cascade.1704.D (3), Casper (1), Catherine.1365 (3), CeCe.1998 (6), CLI&HLT.1345 (6), Cliff.1313 (3), Coffeeshop (2), Continua.502.B (3), Cosenza.3205 (2), Coyote.1103 (3), Crazy_Frog.1477 (3), Crazy_Lord.437 (2), Cruncher (2), Cybercide.2299 (3), Danish_Tiny.163.A (1), Danish_Tiny.333.A (1), Dark_Avenger.1449 (2), Dark_Avenger.2100.A (2), Dark_Revenge.1024 (3), Datacrime (4), Datacrime_II (2), Datalock.920.A (3), DBF.1046 (2), Dei.1780 (4), Despair.633 (3), Destructor.A (1), Diamond.1024.B (1), Dir.691 (1), DOSHunter.483 (1), DotEater.A (1), Ear.405 (3), Eddie-2.651.A (3), Eight_Tunes.1971.A (1), Enola_Gay.1883 (4), F-You.417.A (1), Fax_Free.1536.Topo.A (1), Fellowship (1), Feltan.565 (3), Finnish.357 (2), Fisher.1100 (1), Flash.688.A (1), Four_Seasons.1534 (s), Frodo.3584.A (2), Fumble.867.A (1), Genesis.226 (1), Green.1036 (6), Greetings.297 (2), Greets.3000 (3), Halloechen.2011.A (3), Hamme.1203 (6), Happy_New_Year.1600.A (1), HDZZ.566 (3), Helga.666 (2), HLLC.Even_Beeper.A (1), HLLC.Halley (1), HLLP.5000 (5), HLLP.7000 (5), Horsa.1185 (3), Hymn.1865.A (2), Hymn.1962.A (2), Hymn.2144 (2), Hypervisor.3128 (5), Ibqqz.562 (3), Icelandic.848.A (1), Immortal.2185 (2), Internal.1381 (1), Invisible.2926 (2), Itavir.3443 (1), Jerusalem.1607 (3), Jerusalem.1808.CT.A (4), Jerusalem.Fu_Manchu.B (2), Jerusalem.PcVrsDs (4), John.1962 (3), Joker (1), July_13th.1201 (1), June_16th.879 (1), Kamikaze (1), Kela.b.2018 (3), Kemerovo.257.A (1), Keypress.1280 (6), Kranz.255 (3), Kukac.488 (1), Leapfrog.A (1), Leda.820 (3), Lehigh.555.A (1), Liberty.2857.A (5), Liberty.2857.D (2), Little_Brother.307 (1), Loren.1387 (2), LoveChild.488 (1), Lutil.591 (3), Maresme.1062 (3), Metabolis.1173 (3), Mickie.1100 (3), Necropolis.1963.A (1), Nina.A (1), November_17th.768.A (2), NRLG.1038 (3), NutCracker.3500.D (5), Omud.512 (1), On_64 (1), Oropax.A (1), Parity.A (1), Peanut (1), Perfume.765.A (1), Phantom1 (2), Phoenix.800 (1), Pitch.593 (1), Piter.A (2), Pixel.847.Hello (2), Pizelun (4), Plague.2647 (2), Poison.2436 (1), Pojer.4028 (2), Positron (2), Power_Pump.1 (1), Prudents.1205.A (1), PS-MPC.227 (3), PS-MPC.545 (6), Quark.A (1), Red_Diavolyata.830.A (1), Revenge.1127 (1), Riihi.132 (1), Rmc.1551 (4), Rogue.1208 (6), Saturday_14th.669.A (1), Screaming_Fist.927 (4), Screen+1.948.A (1), Semtex.1000.B (1), Senorita.885 (3), Shake.476.A (1), ShineAway.620 (3), SI.A (1), SillyC.226 (3), SillyCR.303 (3), SillyCR.710 (3), Sofia.432 (3), Spanz.639 (2), Stardot.789.A (6), Stardot.789.D (2), Subliminal (1), Suomi.1008.A (1), Suriv_1.April_1st.A (1), Suriv_2.B (1), Surprise.1318 (1), SVC.1689.A (2), Svin.252 (3), Svir.512 (1), Sylvia.1332.A (1), SysLock.3551.H (2), TenBytes.1451.A (1), Terror.1085 (1), Thanksgiving.1253 (1), The_Rat (1), Tiny.133 (1), Tiny.134 (1), Tiny.138 (1), Tiny.143 (1), Tiny.154 (1), Tiny.156 (1), Tiny.158 (1), Tiny.159 (1), Tiny.160 (1), Tiny.167 (1), Tiny.198 (1), Todor.1993 (2), Traceback.3066.A (2), TUQ.453 (1), Untimely.666 (3), V2P6 (1), V2Px.1260 (1), Vacsina.1212 (1), Vacsina.1269 (1), Vacsina.1753 (1), Vacsina.1760 (1), Vacsina.1805 (1), Vacsina.2568 (1), Vacsina.634 (1), Vacsina.700 (2), Vbasic.5120.A (1), Vcomm.637.A (2), VCS1077.M (1), VFSI (1), Victor (1), Vienna.583.A (1), Vienna.623.A (1), Vienna.648.Lisbon.A (1), Vienna.Bua (3), Vienna.Monxla.A (1), Vienna.W-13.507.B (1), Vienna.W-13.534.A (1), Vienna.W-13.600 (3), Virogen.Pinworm (6), Virus-101 (1), Virus-90 (1), Voronezh.1600.A (2), Voronezh.600.A (1), VP (1), Warchild.886 (3), Warrior.1024 (1), Whale (1), Willow.1870 (1), WinVir (1), WW.217.A (1), XWG.1333 (3), Yankee_Doodle.1049 (1), Yankee_Doodle.2756 (1), Yankee_Doodle.2901 (1), Yankee_Doodle.2932 (1), Yankee_Doodle.2981 (1), Yankee_Doodle.2997 (1), Zero_Bug.1536.A (1), Zherkov.1023.A (1).

**Polymorphic Test-set. 11,000 samples; 500 each of the following 22 viruses:**

Alive.4000, Anarchy.6503, Code.3952:VICE.05, Cordobes.3334, Digi.3547, DSCE.Demo, Girafe:TPE, Gripe.1985, Groove and Coffeeshop, MTZ.4510, Natas.4744, Neuroquila.A, Nightfall.4559.B, One_Half.3544, Pathogen:SMEG.0_1, PeaceKeeper.B, Russel.3072.A, SatanBug.5000.A, Sepultura:MtE-Small, SMEG_v0.3, Tequila.A, Uruguay.4.

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**

# PRODUCT REVIEW 1

## For your D-FENCE?

Dr Keith Jackson

*D-FENCE* from *Sophos* is different from the scanners and checksummers usually covered in *VB* reviews. In addition to authorisation features, *D-FENCE* v4 offers hard- and floppy-disk encryption facilities. Diskette authorisation prevents users accessing unauthorised diskettes, and the encryption features render data inaccessible to those without the appropriate password. *D-FENCE* was provided for review on a single 1.44MB disk.

### Documentation

The documentation comprised a 92-page A5 manual; well-indexed, with an excellent glossary. The manual provides a concise explanation of available facilities, and does not resort to spurious technical terms. It also strongly recommends that *D-FENCE* is first installed in non-encrypting mode. Once a disk is encrypted, it is nigh on impossible to recover data once a problem arises: if this were not true, the encryption used would probably not be worth having.

### Installation and Deinstallation

First, all files on the original *D-FENCE* floppy are copied to any hard disk subdirectory. Then a blank diskette must be formatted, made bootable for DOS (using the SYS command), and all the *D-FENCE* files are copied from the hard disk subdirectory to the root directory of this floppy disk.

Before *D-FENCE* is installed, the manual cautions that the PC should be cold-booted from a write-protected floppy disk, and virus-scanned. An option is available to enforce this. Installation is then merely a matter of booting each PC from this floppy, and using the options provided.

When I tested installation (without encryption), the PC went off for a 15-second 'think' when installation commenced. When this was complete, the program stated that it was examining DFENCE.EXE and again went off for a think (20 seconds this time). After the PC was rebooted, *D-FENCE* had been correctly installed. Unless a disk was encrypted, the time taken to install *D-FENCE* seemed to remain the same.

This describes how *D-FENCE* is installed without using hard-disk encryption. The documentation rightly insists that this is used first as a compatibility test. Once *D-FENCE* has been proven to operate correctly under these circumstances, it can be de-installed, then re-installed using encryption.

Installation with encryption required that the entire hard disk was encrypted, which obviously took much longer (see below). Deinstallation took the same amount of time (decryption is just as slow as encryption!). *D-FENCE* can also be installed onto device drivers – the manual is unclear on this point; however, it transpires that it is able to modify the driver itself to allow *D-FENCE* to use other storage devices.

Deinstallation when encryption has been used should have more 'Are you sure' messages – when deinstallation from an encrypted PC is selected, it commences immediately, putting a message on the screen reading 'Please do not interrupt'. If the power is cut during this process, *D-FENCE* will be able to determine where the encryption was halted and recover accordingly – a particularly handy feature on portables!

### Modes of Operation

*D-FENCE* has five basic modes of operation: Import Control, Import/Export Control, Encrypt hard disks + use DOS floppy disks, Encrypt hard disks + use Import/Export floppy disks, Encrypt both hard and floppy disks.

Import control means any floppy used on a PC protected by *D-FENCE* can only be accessed if 'authorised', a process usually only permitted at 'gateway' PCs (access to which should be controlled). *D-FENCE* rewrites the floppy in a '*D-FENCE* format' (no details supplied). This format does not prevent disks imported onto a PC controlled by *D-FENCE* being read by an 'ordinary' PC. Export control means converted disks must be deauthorised on a gateway PC before they are once again readable on PCs without *D-FENCE*.

> *"D-FENCE provides an effective barrier to prevent introduction of an unauthorised floppy disk"*

When encryption is introduced, a password must be correctly entered before the DOS boot process is allowed to begin. Without the password, the hard disk is inaccessible. A version available for government use has a UK government algorithm which requires two passwords to be entered before a DOS reboot may take place.

The features provided can control PC access, and whether data may be imported or exported to/from the PC – a powerful tool for circumstances that demand such controls.

### Using D-FENCE

When *D-FENCE* is set up, an ID and group name should be specified (maximum 128 characters). The key management provided allows users with the same ID to interchange disks freely. The group name is displayed every time *D-FENCE* executes. Thus, it is possible to set up several *D-FENCE* groups where members of the same group can interchange information, but are debarred from handing information to people outside the group. Different projects perhaps?

A *D-FENCE*-protected PC looks like an ordinary PC, with the exception that a bootup password may be requested. When *D-FENCE* detects an attempt to access an unauthorised diskette, it displays the message 'Unauthorised floppy disk' onscreen. The message can be changed if desired.

When installed, *D-FENCE* manipulates the hard disk's Master Boot Sector to ensure that, even if a floppy boot is performed, the hard disk cannot subsequently be accessed.

The product can be set up so diskette drive access is denied, preventing programs accessing the floppy disk drive at a low level and bypassing *D-FENCE*. No matter what I did during testing, *D-FENCE* prevented access to unauthorised floppy disks. I found no way round the protection that it offered.

When a desired setup has been reached, the configuration can be 'frozen': junior staff can implement *D-FENCE* on a PC, without being able to alter the setup. An excellent feature.

### Memory

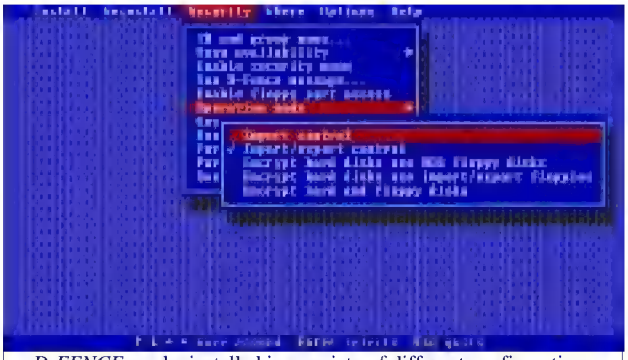
When *D-FENCE* is installed for DOS alone, it does not alter files, only making changes to the boot sector (presumably) of the test PC. When *D-FENCE* subsequently executes, it occupies 3KB of memory: as this is taken before DOS boots, it does not appear on lists of programs which occupy memory.

I measured the amount of RAM *D-FENCE* uses by executing CHKDSK with and without *D-FENCE* present. Without *D-FENCE*, total available memory was 655360 bytes, and, after booting, 628368 bytes were available for program execution. With *D-FENCE*, total available memory reduced to 652288 bytes – 625296 were available for execution.

The difference in both cases was 3072 bytes, exactly 3KB. *D-FENCE* is sparing in its use of RAM, and, unless *Windows* components are invoked (see below), *D-FENCE* does not execute memory-resident programs which occupy low memory.

### Overhead

I tested the overhead of having *D-FENCE* active by timing how long it took to copy 25 files (1.25MB) from one subdirectory to another on the hard disk of my test PC, and also on to the root directory of a 1.44MB floppy disk. I also timed how long it took to boot the test PC (from the hard disk). The tests were carried out with the test PC in various states: without *D-FENCE*, with *D-FENCE* in Import mode, in Import/Export mode, with hard disk encryption and DOS floppy disks, and encrypting both hard and floppy disk.



*D-FENCE* can be installed in a variety of different configurations to suit most systems.

Without *D-FENCE*, copying the test files to floppy took 2 minutes 4 seconds. This test time remained the same with *D-FENCE* installed in Import mode, but rose to 2 minutes 25 seconds with *D-FENCE* installed in Import/Export mode. When floppy disks were encrypted, the test time rose further to 2 minutes 51 seconds; a worst case overhead of 38%.

As long as hard disk encryption was not installed, the set of test files could be copied to a subdirectory of the hard disk in 22 seconds. This time rose to 1 minute 18 seconds when the hard disk was encrypted; a whopping overhead of 250%.

Rebooting the test PC without *D-FENCE* took 33 seconds, rising to 35 seconds with *D-FENCE* installed in Import or Import/Export mode, and increasing further to 49 seconds (a 40% increase) with the hard disk encrypted by *D-FENCE*.

No matter how the figures are dressed up, the overhead is significant, especially when the hard disk is encrypted. As the encryption is carried out in software, this overhead obviously becomes less visible if a more powerful processor is used. However, there will always be a significant overhead involved in using *D-FENCE* to encrypt a hard disk, even on the most powerful PC – for strong crypto, however, this is unsurprising.

The same arguments apply to floppy disk encryption. Here, the measured overhead is greater than that measured for hard disk. However, it probably matters less: floppy disks are slow anyway, so making them slower does not show up as readily; also, diskettes are normally used less frequently than the hard disk, so any imposed overhead is less significant.

### Windows Operation

Extra installation is needed to see *D-FENCE* popup messages whilst *Windows* is running. This process places three files (DFWINSUP.COM, DFPOPUP.EXE and DFPOPUP.DLL) in a fixed subdirectory (C:\DEFENCE), alters AUTOEXEC.BAT to load DFWINSUP at boot time, and adds a line to WIN.INI which loads DFPOPUP when *Windows* is executed.

*Windows* installation also creates DFPOPUP.INI, a control file containing a message (editable as desired) displayed when an unauthorised floppy is detected. *D-FENCE* can also install a 32-bit device driver: I did not try this, as *Toshiba* warns against using such drivers on their 'early' laptops when resume is enabled (as on my test PC).

I encountered problems using *D-FENCE* with *Windows* from the outset: *Windows* would load, then, just as it should be available for use… lockup. The manual states that on 'All Toshiba laptops' there is a known problem where 'Windows displays starting screen then drops back to DOS prompt'. The manual describes how to fix the problem, but I never saw it: my *Toshiba* just hung at the end of the *Windows* load process.

I traced these problems to the line *D-FENCE* had placed into AUTOEXEC.BAT. This was the last line of the file; however, the manual does not state that this file would be altered. The multiple-boot scheme employed on my PC ensured that the line pertaining to DFWINSUP was never executed. Once this line was moved to a more suitable location, and the PC rebooted, *Windows* was available. DFPOPUP could now make the 'Unauthorised floppy disk' message visible onscreen.

Even having solved the problems outlined above, using the test PC under *Windows* still produced intermittent lockup problems. Three times when *D-FENCE* was installed, *Windows* would die and require a complete reboot. I never traced the problem. Without *D-FENCE* it never happened.

Starting *Windows* without *D-FENCE* took 43 seconds, and 1 minute 2 seconds (a 44% increase) when the hard disk of the test PC was encrypted. As *Windows* startup requires a lot of disk activity, this overhead is hardly surprising.

*Sophos* states that the product works perfectly well under *Windows*; however, a PC with more modern specifications is preferable.

### Encryption and Purging

As well as preventing access to unauthorised floppy disks, *D-FENCE* can encrypt (and/or decrypt) a floppy and/or a hard disk. Encrypting the entire content of a hard disk takes some time – 23 minutes 14 seconds on my test PC. *D-FENCE* took 2 minutes 36 seconds to encrypt a 1.44MB floppy.

No details are provided in the documentation of what type of encryption *D-FENCE* uses – having said that, high-end users would wish to examine the algorithm to ensure security, and others would not be able to verify it anyway.

Users can evade *D-FENCE* by deleting a floppy disk file, importing the floppy disk into a PC controlled by *D-FENCE*, and then undeleting the file. This can be prevented by making *D-FENCE* purge (overwrite) all erased space on a floppy when either an import or an export action is performed.

Three levels of purge are provided: 'Standard' overwrites the empty space once, 'Government' performs three overwrites then verifies the purged space, and 'Military' performs seven overwrites, then verifies. Repetitive overwrites are provided because it is possible (under lab conditions) to read data previously stored on the disk (by reading from the margins of the 'normal' track). Multiple overwrites reduce the chances of retrieving information using such a process to almost zero.

Purging of erased space is a slow process, and should not be introduced in circumstances where such an overhead is undesirable. I measured how long it took *D-FENCE* to 'purge' a full floppy disk (the minimum time), and an empty floppy disk (the worst case time), for various security levels.

Using 'Standard' security, a full disk could be purged in 17.0 seconds, rising to only 17.3 seconds when a higher security level was used. When an empty floppy disk was used, purge time rose to 1 minute 49 seconds for 'Standard' security, 6 minutes 20 seconds for 'Government' level security, and 12 minutes 53 seconds for 'Military' level security.

Confirmation measurements were made on partially full disks, and there is no doubt that the above measurements reflect quite accurately the time needed to purge the empty space on a floppy disk when 'Imported' by *D-FENCE*. Given all these figures had increased from a base timing of 17 seconds, the extra time needed in all cases is onerous.

### The Rest

A program called DFTEST is provided which is intended to test whether *D-FENCE* is currently running on a PC. When DFTEST is executed, nothing appears on-screen apart from a startup message. By default, any problems are reported only by returning an ERRORLEVEL (which can be interrogated in a batch file). However, it is possible to make the program report its results on-screen by using a command-line parameter.

A utility called PASSWORD is provided which, not surprisingly, can be used to set a new *D-FENCE* password.

### Conclusions

In this review I have tried to explain the features offered by *D-FENCE*, and to measure what overhead it introduces when it is present.

*D-FENCE* provides an effective barrier to prevent introduction of an unwanted (unauthorised) floppy disk. As with any such product, potential users should look carefully at the overhead imposed, which is, of course, noticeable. On more modern computers, the overhead will be less intense, due to higher processor speeds; however, it would be foolish to expect a sector-level crypto utility not to affect performance.

P.S. The phone number contained inside DFENCE.EXE still uses UK dialling code 0235 rather than 01235, which it has been for at least a year now. My consultancy fee invoice for debugging is in the post!

**Technical Details**

**Product:** *D-FENCE v4.09* (no serial number visible).

**Developer/Vendor:** *Sophos Plc*, The Pentagon, Abingdon, Oxfordshire OX14 3YP, UK. Tel +44 1235 559933, fax +44 1235 559935, email: enquiries@sophos.com.

**Vendor US:** *Sophos Inc*, 18 Commerce Way, Woburn, Massachusetts 01801 USA. Tel +1 617 932 0222, fax +1 617 932 0251.

**Availability:** DOS v3.31 or above (according to the *D-FENCE* documentation), though the error messages within the EXE files only refer to DOS version 3.

**Price:** Single user – £245. Site licences from £49.50 per computer; comprehensive pricing available on application to the company.

**Hardware used:** *Toshiba 3100SX*, a 16MHz 386 laptop with 5MB RAM, a 3.5-inch (1.44M) floppy disk drive, and a 40MB hard disk, running under *MS-DOS v5.0*.

# PRODUCT REVIEW 2

## LANDesk Virus Protect for Windows NT

Martyn Perry

This review takes a look at *LANDesk Virus Protect* v1.70, *Intel's* offering for the *Windows NT* environment. This review focuses on the package's *NT* components, and particularly their functionality under *NT 4.0*. *Intel* provided us with its 45-day 'test-drive' CD-ROM: this allows evaluation of *LANDesks* for *Windows 3.1x*, *Windows 95*, *Windows NT*, and *NetWare* – documentation for each is also included on the CD. The licence for the full version is granted for use on one server with unlimited clients.

### Presentation and Installation

For this review, only the CD-ROM mentioned above was shipped. The *Adobe Acrobat* reader software is included on the CD, and the *Acrobat* file containing the manual occupies just under 729KB for the 68-page document.

Installation is performed from the CD-ROM. As *NT 4.0* supports AutoPlay, the user is automatically dropped into the setup program; under previous versions it is necessary simply to run SETUPVP.EXE. The opening screen allows the user to choose which product to install. Once the selection is made, licence information is displayed: after the user has agreed to its conditions, installation begins.

First, the destination directory (the default under *NT 4.0* is C:\Program Files\Intel\LANDesk\VProtect) for the 9.53MB of program files is selected. Next, installation asks whether a personal or common program group should be created. This is followed by the selection of initial system defaults for:

- Action on discovery of a virus: rename with extension VIR, Move to SUSPECT directory (default), Leave alone, or Delete
- Real-time scan selection: incoming (modified) default, incoming/outgoing, or off

Next, there is a request for a valid licence number: for the 45-day test-drive, this is left blank. The files are then copied to the selected drive and the relevant program group created. Finally, the installer is asked if he wishes to install the *Acrobat* reader to read the PDF documentation files on the CD-ROM. This can be skipped if *Acrobat* is present. The user is also prompted to examine README.TXT for the latest information.

### Getting Started

The product is shipped with client support for *Windows NT*, *Windows 95*, and *Windows 3.1x* using WProtect. DOS clients use VSCAND.EXE. *LANDesk* itself has three scan types: Manual, Scheduled and Real-time.

A Manual Scan can be run from the tools options on the main menu, or from the toolbar. Once running, the scan monitor displays the progress of the scan – elapsed time and percentage of scan completed, and also the location and name of the last virus found.

A test file, VPTEST, is provided: this is a dummy virus which can be used safely to test the actions of various scanner configurations. The scanner can be stopped part way through a scan: hitting stop produces a dialog box which gives the user the chance to allow the scan to continue – this doubles as a pause option.

Under the Virus Information window is a list of any viruses found, along with associated locations. This list can be scrolled while the scanner is running. At the end of the scan, the action buttons are enabled: the options are Clean, Delete, Rename, and Move, and files can be selected individually or en masse. This provides flexibility where an administrator wants to clean a known infection but may wish to move a new infection to the quarantine directory for further investigation.

Scheduled scans can be run daily, weekly, or monthly. The 'No Scan' option allows a configuration to be set up but not activated until required – when the time comes, the scan time option is all that must be changed. The scheduled configuration includes the same selections as the manual scan; the action selections are delete, move and rename.

The scheduler handles only one scan at a time and does not allow scans to queue if one is in operation when a second is due – perhaps a little primitive? In addition, a scheduled scan cannot be stopped: it is necessary to go to the *NT* Task Manager and end the task – which, of course, kills the whole program.

A real-time scan can be configured for incoming files and file renaming only (the default), incoming and outgoing files, or deactivated completely. The real-time scan can be disabled at any time by clearing both Incoming and Outgoing options, and the actions available on virus detection are delete, rename and move. If 'move' is the action selected for real-time scan, it uses the same quarantine directory as for the manual scan.

### Administration

No additional password is required to access the scanner administration configuration: the main menu gives access to the various options, which include:

- File types – either all files or those included in the extension list. The default file extensions are COM, DOC, DOT, EXE, TMP and XLS. Additional file extensions can be added as required.
- Areas to be scanned – either all drives and directories or selected drives and directories

- Action on detecting a virus – move (transfer to quarantine directory, rename (changes file extension), leave alone (no action taken), delete (removes the file)

Extra options include expansion of compressed executable and zipped files, and scanning for mutation (polymorphic) viruses and boot sector viruses. All these are selected by default.

### Reports, Activity Logs, and Updates

*LANDesk* provides several options for notification on virus discovery. The message issued can be user-configured, and can also inform the recipient what action was taken, which may save the alerted user from having to access the main server running the scan program. The options are:

- Message Box – notifies a computer by displaying a message box, issuing a beep, or displaying the message with an accompanying .WAV file. If this option is selected, the sound plays till the message box is closed, ensuring that someone takes notice of the warning.
- Run Program – allows a program to be run. This could be a Fax program, since this option is not included.
- Numeric Pager – uses a connected modem to contact a paging service
- Printer – allows a printed message to be displayed on a designated printer
- Alpha Pager – uses a connected modem to contact a paging service
- Internet Mail – uses SMTP to send warnings

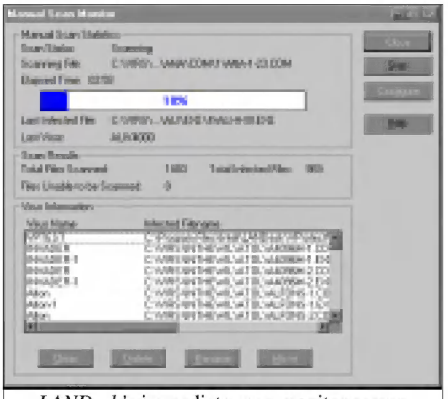
There is also support for SNMP traps, using an Event Forwarder, which watches event logs for specified events. The *NT* event logs record system, security and application events. The configured notification set-up can be deployed to other machines using cut and paste – curiously, this only works on up to 10 PCs at a time.

*LANDesk* provides a listing of virus patterns. The information provided includes the virus type and advises whether or not it can be cleaned. The virus encyclopædia can also be selected; this provides additional notes relating to each specific virus.

*Intel* operates an automated download of virus signatures from its BBS. The same BBS or the Internet can be used for on-demand download of the virus list. Separately, *Intel* runs a list server, an automated Internet email notification service to provide *LANDesk* users with updates on new viruses, maintenance release files, etc.

### Detection Rates

The scanner was run against the usual *VB* test-sets: In the Wild File, In the Wild Boot Sector, Standard and Polymorphic (see the summary for table details). Tests were conducted using default scanner file extensions. The scan action option was set to move infected files, and the residual file count was used to determine the detection rate. During testing, the Application event log was filling quickly due to the large number of virus detections. The setting was originally set for a fixed length of 512KB. This kept giving errors and was changed to allow the Event Log to wrap. The scan was re-run and again slowed down about two-thirds of the way through the polymorphic samples, again producing an 'Out of Virtual Memory' error.



*LANDesk's* immediate scan monitor screen offers the usual set of controls.

The problem seems to be with holding so many entries in the scan monitor whilst performing the scan. This also has an impact on the scan speed as additional entries are added to the bottom of the growing table, causing the machine to page excessively. Bear in mind that these tests were performed essentially without any other major application running; but also the 16MB of memory is very low for such a machine.

It could easily be argued that the *VB* test-set (over 12,000 virus-infected files) is a more severe test than would be experienced in a normal work environment. This may be valid for workstations, but it is easy to imagine a situation where a single server has thousands of files infected.

The results were variable. The score against the Polymorphic test-set was 94.4%: the problem was that the scanner could not detect any of the 500 Anarchy samples and about one-quarter of the samples of Gripe.1985. The In the Wild test achieved a tolerable 89.7%. However, the product struggled in the Standard test, scoring 66.0% across a range of viruses.

### Real-time Scanning Overhead

To determine the impact of the scanner on the machine, we timed how long it took to copy 200 files of 20.55MB (EXE and COM files) from one directory to another using XCOPY. The source and target directories were excluded from any immediate scan to avoid the risk of a clash. The default setting of Maximum Boost for Foreground Application was used for consistency in all cases.

Because of the different processes which occur within the server, the timing tests were run ten times for each setting, and an average taken. The tests (see summary for detailed results) were:

- Program not loaded: this establishes the baseline time for copying the files on the server
- Program unloaded: this is run after the other tests to check how well the server is returned to its former state

- Program loaded; Real-time scan incoming and outgoing both off, and the immediate scanner not running: this tests the impact of the application in a quiescent state
- Program loaded with Real-time scan on incoming only, but the immediate scanner not running: this tests the impact of the incoming scan on its own
- Program loaded with Real-time scan incoming and outgoing, again with immediate scan off: this shows the full overhead of the real-time scans
- Program loaded; Real-time scan incoming/outgoing and immediate scan running: this is the full impact of running real-time and immediate scanners on files

As usual, the tests show the real-time scan overhead is best managed by selecting only 'incoming'. During timing tests, if the program was unloaded with the real-time scan still selected, overhead was the same as if the program was still running. If these options are disabled, the overhead is removed.

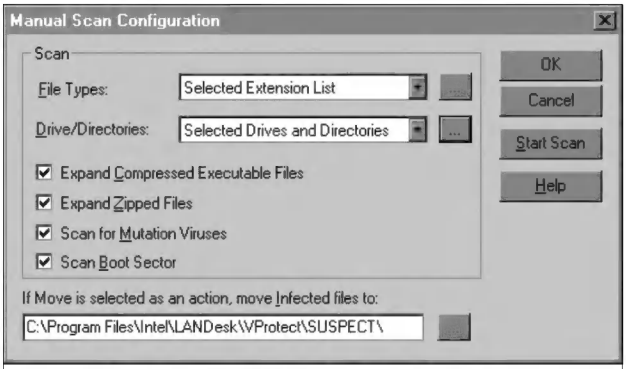
### Summary

Installation was easy, with good information provided to explain what is happening. This was good to see, as the *NetWare* version of the product has had in the past a convoluted installation procedure which deposited files in multiple directories. There is an uninstall facility for removing the product, if this should become necessary.

The facility to set the configuration for the real-time scan during installation provides for immediate protection of the server. The various software elements are well integrated into the *NT* environment. It is good to see that the scheduled scan is an integral part of the application and use is made of the *NT* logs. The virus reporting options are comprehensive. The automated signature download seems to be a feature more developers are providing, and the product has a good professional feel, providing also multiple server support.

The scanner results, although reasonable against the In the Wild and the Polymorphic test-sets, were unimpressive for the Standard tests.

Overall, *Intel* has added a product to its *LANDesk* range which compares favourably with their more established *NetWare* product.




The configuration section for manual scans.

## Intel LANDesk Virus Protect for NT

Detection Results

| Test-set[1] | Viruses Detected | Score |
|---|---|---|
| In the Wild File | 472/476 | 99.2% |
| In the Wild Boot | 69/86 | 80.2% |
| In the Wild Overall | – | 89.7% |
| Standard | 351/532 | 66.0% |
| Polymorphic | 10382/11000 | 94.4% |

Overhead of On-access Scanning:

The tests show the time taken to copy 200 COM and EXE files (20.55MB). Each test is performed ten times, and an average is taken.

| | Time | Overhead |
|---|---|---|
| Program not loaded | 25.3 | – |
| Program unloaded | 25.5 | 1.0% |
| Program loaded<br>Incoming OFF<br>Outgoing OFF<br>No Manual Scan | 26.3 | 3.9% |
| Program loaded<br>Incoming ON<br>Outgoing OFF<br>No Manual Scan | 42.3 | 67.4% |
| Program loaded<br>Incoming ON<br>Outgoing ON<br>No Manual Scan | 57.0 | 25.3% |
| Program loaded<br>Incoming ON<br>Outgoing ON<br>Manual Scan | 74.8 | 96.0% |

**Technical Details**

**Product:** *Intel LANDesk Virus Protect v1.70, VPN v250.*

**Developer US:** *Intel Corp*, 734 East Utah Valley Drive, Suite 300, American Fork UT 84003-9773. Tel +1 801 828 3000.

**Developer UK:** *Intel Corp*, Pipers Way, Swindon SN8 2BS, Wiltshire. Tel +44 1793 403000, fax +44 1793 488013.

**Price:** One server + clients US$1495
four servers + clients US$5180
twenty servers + clients US$21,900

*Intel* has a flexible licensing agreement, allowing an organization to install client scanners on any workstation connecting to an *LDVP*-protected server. Users can also have the product on their home PCs at no extra cost. Upgrades can be purchased; however, they are free if an organization purchases a Software Maintenance Agreement.

**Hardware Used:** *Compaq Prolinea 590* with 16MB RAM and 2GB of hard disk, running *NT 4.0* workstation with Service Pack 1.

[1]Test-sets: For In the Wild file, Standard, and Polymorphic listings, see this issue; p.17. In the Wild boot sector viruses are listed in the January 1997 edition of *Virus Bulletin*; see p.17.

**SUBSCRIPTION RATES**

**Subscription price for 1 year (12 issues) including first-class/airmail delivery:**

UK £195, Europe £225, International £245 (US$395)

**Editorial enquiries, subscription enquiries, orders and payments:**

*Virus Bulletin Ltd*, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

June Jordan, *Virus Bulletin*, 590 Danbury Road, Ridgefield, CT 06877, USA

Tel +1 203 431 8720, fax +1 203 431 8165



# END NOTES AND NEWS

***Sophos Plc's* next round of anti-virus workshops** will be on 19/20 March 1997 at the training suite in Abingdon, UK. The company's training team is also hosting a Practical *NetWare* Security course on 13 March 1997 (cost £325 + VAT). Information is available from Julia Edwards, Tel +44 1235 544028, fax +44 1235 559935, or access the company's World Wide Web page; http://www.sophos.com/. The company has also announced the release of InterCheck for *Windows NT*: contact Petra Duffield (email pd@sophos.com) for information.

***InfoSecurity 1997*** will take place at Olympia 2 (London, England) from 29 April–1 May 1997. The event is planned to address all aspects of IT security in the business environment, and many anti-virus developers will be present. For information, contact Yvonne Eskenzi on Tel +44 181 449 8292, or on the Web at http://www.infosec.co.uk/.

***Reflex Magnetics* is presenting 'The Hacking Threat'** from 4–6 March 1997. The venue for both is *Reflex's* premises in London, England. For further information, contact Phillip Benge at *Reflex Magnetics*; Tel +44 171 372 6666.

***IBM* has announced the appointment of Sarah Gordon and her husband Richard Ford** to its anti-virus staff. Ford (one-time editor of *Virus Bulletin*) and Gordon previously worked for *Command Software*, and will be part of a team of anti-virus experts and professional developers at the company's TJ Watson Research Center.

*Symantec* has released *Norton Internet Email Gateway*, designed to **intercept viruses within SMTP email attachments**. The product scans inside ZIP, UUENCODE and MIME files, and free updates are provided automatically from the *Symantec* AntiVirus Research Center. The company has also announced the launch of Bloodhound, 'a revolutionary new system which uses the latest artificial intelligence technology to scour the World Wide Web searching for new and unknown computer viruses', according to a press release. The technology is said to use artificial intelligence to detect the presence of virus-like behaviour. For information on these, and other, *Symantec* products, visit the company's WWW site; http:///www.symantec.com/.

***SecureNet 97* will take place on 20/21 March 1997 in Cannes, France**; speakers include such well-known anti-virus 'names' as Fred Cohen, Vesselin Bontchev, Klaus Brunnstein, and Eugene Spafford. Information is available from Alex Verhoeven at *Elsevier Advanced Technology*; Tel +44 1865 843654, fax +44 1865 843971, email a.verhoeven@elsevier.co.uk.

*Dr Solomon's Software Ltd* (formerly *S&S International*) is presenting **Live Virus Workshops** at the *Hilton National* in Milton Keynes, Buckinghamshire, UK on 25/26 March 1997. Details from Melanie Swaffield at *Dr Solomon's*; Tel +44 1296 318700, Web site http://www.drsolomon.com/.

***CeBIT 97*, billed as the premier international trade fair for the information technology and communications industry**, will take place in Hannover from 13–19 March 1997. This year's display categories are: office technology, information technology, software, network computing, telecommunications, bank technology, card and security technology, computer integrated manufacturing and computer aided research, and technology transfer. For more detailed information on the event, email cebit@hfusa.com.

The **1997 *DECUS* conference will take place from 7–10 April** at the University of Westminster in the UK. The event will cover a wide range of topics, and, in addition to the presentations, delegates will also be able to attend various half- and full-day seminars. For information, contact the *DECUS* registration line; Tel +44 118 920 2182, fax +44 118 920 2211.